

مقدمة قصيرة جدًّا

علم التشفير

فريد بايبر وشون ميرفي

علم التشفير

علم التشفير

مقدمة قصيرة جدًّا

تأليف
فريد بايبر وشون ميرفي

ترجمة
محمد سعد طنطاوي

مراجعة
هاني فتحي سليمان

مراجعة علمية
د. حاتم بهيج



علم التشفير

Cryptography

فريد بايبر وشون ميرفي

Fred Piper and Sean Murphy

الطبعة الأولى ٢٠١٦م
رقم إيداع ٢٠٧٤٩ / ٢٠١٣

مؤسسة هنداوي للتعليم والثقافة
إن مؤسسة هنداوي للتعليم والثقافة غير مسئولة عن آراء المؤلف وأفكاره
وإنما يعبِّر الكتاب عن آراء مؤلفه
٥٤ عمارات الفتح، حي السفارات، مدينة نصر ١١٤٧١، القاهرة
جمهورية مصر العربية
تليفون: ‎+ ٢٠٢ ٢٢٧٠٦٣٥٢ **فاكس:** ‎+ ٢٠٢ ٣٥٣٦٥٨٥٣
البريد الإلكتروني: hindawi@hindawi.org
الموقع الإلكتروني: http://www.hindawi.org

بايبر، فريد.
علم التشفير: مقدمة قصيرة جدًّا/تأليف فريد بايبر، شون ميرفي.
تدمك: ٥ ٥٢٢ ٧١٩ ٩٧٧ ٩٧٨

١- الشفرة
٢- الكتابات السرية

أ- ميرفي، شون (مؤلف مشارك)
ب- العنوان

٦٥٢,٨

تصميم الغلاف: إيهاب سالم.

المحتويات

شكر وتقدير

تشكَّلت ملامحُ هذا الكتاب على مدار سنواتٍ عدَّةٍ ساهم خلالها كثيرون بتعليقاتهم واقتراحاتهم القيِّمة. نتقدَّم بخالص الشكر إليهم جميعًا. نتوجَّه بالشكر على وجه الخصوص إلى جيري كول، وروس بتل، وبيتر وايلد لقراءة المُسوَّدة النهائية، وإلى أدريان كالي، وكالاتزس نيكولاس لإعفائنا من الحرج؛ وذلك من خلال تصويب بعض التمارين التي قدَّمناها. كما نتوجه بشكرٍ خاصٍّ إلى بولين ستونر على ما ساهمت به، وعلى نجاحها في تحويل ما بدا كتابةً عشوائيةً غير منسَّقة إلى صورةٍ أنيقة. لقد اختُبر صبرها مراتٍ عديدةً، ولولاها لما خرج الكتاب إلى النور في صورته النهائية.

الفصل الأول

مقدمة

يُحكِم معظم الناس لصق الأظرف قبل إرسال خطاباتهم، وإذا سُئِلوا عن سبب ذلك، فستأتي بعض الإجابات الفورية من قبيل: «لا أعرف حقيقةً» و«مجرد عادة» و«لِمَ لا؟» و«لأن الجميع يفعلون ذلك.» قد تشمل الإجابات الأخرى الأكثر تعقُّلًا إجاباتٍ من قبيل: «لمنع الخطاب من السقوط»، أو «لمنع الآخرين من قراءة الخطاب». حتى في حال لم تحتوِ الخطابات على معلومات حساسة أو شخصية جدًّا، يرى الكثيرون منا أن هناك خصوصية في محتويات مراسلاتنا الشخصية، وأن إحكام لصق الأظرف يمنع اطِّلاع الآخرين عليها باستثناء متلقي الرسائل المقصود. إذا أرسلنا خطاباتنا في أظرفٍ غير مغلقة فسيستطيع أي شخص يحصل على الظرف أن يقرأ محتويات الرسالة. ومسألة ما إذا كانوا سيَقرءُون الرسائل بالفعل أم لا قضية أخرى. المهم أنه ما من شكٍّ في أنهم سيتمكَّنون من قراءتها إنْ هم أرادوا ذلك. بالإضافة إلى ذلك، إذا استبدلوا الرسالة الموجودة داخل الظرف، فلن نعرف أنهم فعلوا ذلك.

يعتبر استخدام البريد الإلكتروني بالنسبة إلى الكثيرين حاليًّا بديلًا لإرسال الخطابات من خلال البريد العادي. والبريد الإلكتروني وسيلة سريعة للتواصل لكِنْ بطبيعة الحال لا توجد أظرفٌ لحماية الرسائل، بل يُقال عادةً إن إرسال الرسائل عبر البريد الإلكتروني يشبه إرسال الخطابات عبر البريد العادي دون أظرف. بداهةً، من يُرِد إرسال رسائل سرية أو مجرد رسائل شخصية عبر البريد الإلكتروني، فسيحتاج إلى وسيلة أخرى لحمايتها. تتمثل إحدى هذه الوسائل في استخدام التشفير وتشفير الرسائل.

إذا وقعت رسالة مُشفَّرة في أيدي أشخاص غير المتلقين المعنيِّين، يجب أن تبدو هذه الرسالة غير مفهومة. لم ينتشر استخدام التشفير لحماية رسائل البريد الإلكتروني على نطاق واسع بعدُ، بَيْدَ أنَّ ذلك يحدث حاليًّا، وعلى الأرجح سيزداد انتشارُه اتساعًا. في

الواقع، تقدَّمت مجموعة من أعضاء البرلمان الأوروبي بتوصيةٍ في مايو ٢٠٠١ بضرورة تشفير جميع مستخدمي أجهزة الكمبيوتر في أوروبا لرسائلهم الإلكترونية بغرض «تفادي تجسُّس شبكة التنصُّت البريطانية-الأمريكية».

التشفير علم راسخ كان له أثرٌ تاريخيٌّ كبيرٌ لأكثر من ألفَيْ عام. جرت العادة أن الحكومات والمؤسسات العسكرية كانت بمنزلة المستخدمين الرئيسيين له، على الرغم من ضرورة الأخذ في الاعتبار أن كتاب فاتسيايانا «كاما سُترا» يحتوي على توصية للنساء بدراسة «فن فهم الكتابة المشفَّرة» (توجد جميع البيانات الكاملة للأعمال المُستشهَد بها في هذا الكتاب في قسمَيِ المراجع والقراءة الإضافية).

وتأثير علم التشفير على التاريخ موثَّقٌ توثيقًا جيدًا. ولا شكَّ في أن المرجع الأساسي حول التشفير هو كتاب «فاكُّو الشفرات» لديفيد كان. يقع هذا الكتاب في أكثر من ألف صفحة ونُشِر للمرة الأولى في عام ١٩٦٧. وُصِف الكتاب بأنه «أول كتاب شامل يروي تاريخ الاتصالات السرية»، وبأنه كتاب ممتع للغاية. في وقت قريب، ألَّف سايمون سينج كتابًا أكثر إيجازًا بعنوان «كتاب الشفرة»، وهو كتاب مبسَّط يعرض بعضًا من أهم الأحداث التاريخية. وفي حين أن هذا الكتاب لا يعتبر كتابًا شاملًا ككتابِ كان، فإنه يهدف إلى إثارة اهتمام القارئ العادي بالموضوع. كلا الكتابين رائع ونوصي بشدة بقراءتهما.

لا يقتصر الفضل في نشر وزيادة الوعي العام بالأهمية التاريخية لعلم التشفير على المؤلفات، بل يمتد إلى عدد من المتاحف والأماكن التاريخية حيث تُعرض ماكينات التشفير القديمة. يأتي على رأس قائمة هذه الأماكن حديقة بلتشلي في إنجلترا التي يعتبرها كثيرون موطنَ علم التشفير والحوسبة الحديثة. في هذا المكان تمكَّن آلان تورينج وفريقه من فكِّ شفرة إنيجما، وحُفِظت بيئة عملهم كأثرٍ تاريخيٍّ لإنجازات تورينج وفريقه المدهشة. أظهر الكثير من الأفلام الحديثة عن الحرب العالمية الثانية أهميةَ فكِّ الشفرة. تتمثل المحطات التاريخية التي تلقَّت اهتمامًا خاصًّا في أثر فكِّ شفرة إنيجما وفكِّ شفرة الرسائل المشفَّرة قبل الهجوم على ميناء بيرل هاربور مباشرةً. خُصِّص أيضًا عددٌ من المسلسلات التليفزيونية لتناول الموضوع. كل هذا يشير إلى اطِّلاع الملايين حول العالم على مفهوم تشفير الرسائل للحفاظ على سرِّيَّتها وعلْمهم بالآثار التي قد تترتب على فكِّ شفرتها. لكنَّ المعنى الدقيق للمصطلحات المستخدمة لا يزال غامضًا بالنسبة إلى الكثيرين منهم، كما لا يزال فهمهم لها محدودًا. يهدف هذا الكتاب إلى إصلاح هذا الوضع من خلال تقديم عرضٍ غير متخصص للتعريف بعلم التشفير؛ فنِّ وعلمِ وَضْعِ وفكِّ الشفرات. وبعد

الانتهاء من قراءة هذا الكتاب سيتمكن القُرَّاء من مشاهدة تلك الكتب والأفلام والمسلسلات التليفزيونية بمزيدٍ من المعرفة، وهذا ما سيجعلها مفهومةً أكثر؛ ومن ثَمَّ أكثر إمتاعًا لهم.

قبل سبعينيات القرن العشرين، كان التشفير فنًّا غامضًا لا يفهمه أو يمارسه سوى حفنةٍ من الأفراد العاملين في الحكومات والمؤسسات العسكرية. وحاليًّا، يُعدُّ التشفير مجالًا أكاديميًّا راسخًا يُدرَّس في العديد من الجامعات، كما يمكن أن تستخدمه الشركات والأفراد على نطاق واسع. كانت هناك عوامل عديدة أثَّرت على هذا التحوُّل. يتمثل العاملان الأكثر وضوحًا في هذا التحول في الاتجاه نحو أتمتة الشركات وظهور الإنترنت كوسيلة اتصال. فالشركات حاليًّا تريد إجراء معاملاتها التجارية بعضها مع بعض، ومع عملائها من خلال الإنترنت. وتريد الحكومات أيضًا أن تتواصل مع مواطنيها من خلال الإنترنت، بحيث يجرى — على سبيل المثال — تقديم الإقرارات الضريبية إلكترونيًّا.

بينما لا يوجد شكٌّ في أن التجارة الإلكترونية تزداد انتشارًا، غالبًا ما يُشار إلى المخاوف الأمنية كإحدى العقبات في طريق الاعتماد عليها اعتمادًا كاملًا. لقد ركزنا بالفعل على المشكلات المرتبطة بالمعلومات السرية، لكن السرية لا تكون عادةً المصدر الرئيسي للقلق.

إذا كان هناك شخصان يتواصلان عبر شبكة عامة ولا يستطيع أحدهما رؤية الآخر، فإنه لا يبدو واضحًا في الحال كيف سيستطيع أيٌّ منهما تحديد هُويَّة الآخر. لكن من الواضح أنَّ مَن يتلقى رسالة عبر شبكةٍ ربما عليه أن يُقنع نفسه بمعرفته بهوية الطرف المُرسل، وبأنه واثق من أن الرسالة التي يتلقاها تتطابق مع الرسالة الأصلية التي جاءته من الطرف المُرسل. بالإضافة إلى ذلك، ربما تكون هناك حالات يحتاج فيها الطرف المتلقي إلى أن يضمن عدم إنكار الطرف المُرسِل لاحقًا للرسالة التي بعثها والادعاء بإرسال رسالة مختلفة. تلك قضايا مهمة ليست يسيرة الحل.

في بيئات العمل التقليدية غير المُؤَتْمَتَة، يجري في كثير من الأحيان الاعتمادُ على التوقيعات المكتوبة يدويًّا لتوفير الضمانات اللازمة إزاء مصادر القلق الثلاثة السابقة. يتمثَّل أحد التحديات الرئيسية التي واجهها المتخصصون في المجال الأمني حديثًا في اكتشاف «مكافِئات إلكترونية» تحل محل الآليات الاجتماعية؛ مثل التعرف على الأشخاص من خلال المواجهة المباشرة والتوقيعات المكتوبة يدويًّا، التي لا يصبح لها مكان عند التحوُّل إلى المعاملات الرقمية. وعلى الرغم من عدم وجود علاقة مباشرة للحاجة إلى الاحتفاظ بسرية بعض المعلومات، صار علم التشفير أداة مهمة في مواجهة هذا التحدي. في بحثٍ نُشر في

عام ١٩٦٧ تحت عنوان «اتجاهات جديدة في التشفير»، اقترَح وايتفيلد ديفي ومارتن هلمان طريقةً قد يُستخدم التشفير فيها لإصدار مكافئ إلكتروني للتوقيعات اليدوية. يستحيل التأكيد بالقدر الكافي على مدى أهمية ذلك البحث. فقبل بحثهما، كان التشفير يُستخدم في جعل المستخدِمين على يقين بأن رسائلهم لم تتبدل أثناء إرسالها. ومع ذلك كان الأمر يعتمد على الثقة المتبادلة بين الطرفين المتراسلَين. لم يكن في ذلك مشكلة بالنسبة إلى المؤسسات المالية، التي ربما كانت المستخدِم الرئيسي للتشفير في ستينيات وسبعينيات القرن العشرين، بَيْدَ أن بيئاتِ وأماكن استخدام التشفير كانت بالتأكيد محدودة.

تطوَّر علم التشفير الحديث تطورًا كبيرًا خلال العقود الثلاثة المنصرمة. لا يقتصر الأمر على تطوُّر التكنولوجيا نفسها، بل امتد ليشمل طيفًا واسعًا من التطبيقات. بالإضافة إلى ذلك، على الأرجح أن يكون الجميع مستخدِمًا مباشرًا للتشفير أو يتأثر باستخدامه؛ لذا، فإننا جميعًا نحتاج إلى فهم آليات التشفير وما يمكن أن تحققه.

(١) طريقة استخدام هذا الكتاب

يقدِّم هذا الكتاب رؤية عامة كمَدخل إلى علم التشفير، وهو مكتوب بِلُغةٍ غير متخصصة ويستهدف القارئ العادي في الأساس. أما علماء الرياضيات والكمبيوتر الذين يرغبون في دراسة الجوانب الفنية للتشفير، فأمامهم الكثير من الخيارات. النظريةُ الأساسية لتصميم وتحليل خوارزميات التشفير موثَّقة توثيقًا جيدًا، فضلًا عن توافر الكثير من الكتب حول هذا الموضوع. (نرى أن المرجع الرئيسي في هذا المجال هو كتاب «دليل علم التشفير التطبيقي» لألفريد مينيزيس وبول فان أورشخوت، وسكوت فانستون.) لكتابنا هذا هدف محدد لا يتعداه إلى غيره؛ فهو لا يركِّز على الجوانب الفنية المصاحبة لتصميم الخوارزميات، بل يركِّز على طرق وأغراض استخدامها. إذا حفَّز هذا الكتابُ القراءَ ذوي الخلفيات الرياضية المناسبة على الاطلاع على كُتب فنية أكثر تخصصًا، فسيكون قد حقق أحد أهدافه. لكن هدفه الرئيسي هو محاولة إزالة الغموض المحيط بالتشفير والتخلص من الخوف الذي ينتاب غير المتخصصين في الرياضيات إزاءه.

يقوم هذا الكتاب على أحد مقررات ماجستير العلوم في الأمن المعلوماتي في كلية رويال هولوواي في جامعة لندن. كان المقرر يحمل اسم «فهم علم التشفير»، ثم تغيَّر عنوانه إلى «مقدمة في علم التشفير وآليات الأمن». وبينما تتنوع اهتمامات وخلفيات طلاب هذا المقرر، يتملك معظمَهم طموحٌ في أن يصبحوا متخصصين عاملين في المجال الأمني،

ويشمل ذلك — على سبيل المثال — العمل كمديري أمنِ تكنولوجيا المعلومات وخبراء للأمن المعلوماتي. لا يرغب معظم هؤلاء في أن يصبحوا متخصصين في مجال التشفير، بل إنهم في واقع الأمر، يختارون هذه المادة وهم ينظرون إلى التشفير كشرٍّ لا بد منه يجب تحمُّله بغرض الحصول على مؤهِّل في أمن المعلومات. وبينما لا نرى نحن، مؤلفا هذا الكتاب، في التشفير «شرًّا»، فإنه يجب دراسة التشفير بالتأكيد في سياق تصميم أنظمة آمنة، بدلًا من اعتباره موضوعًا مستقلًّا قائمًا بذاته. يبرر هذا المنطلقُ الاعتقادَ بأن فهم المشتغلين بالمجال الأمني لكيفية إدارة كلمات السر أكثر أهمية في العموم من قدرتهم على التحليل الرياضي للأنظمة المشفرة.

أما بالنسبة إلى هؤلاء ممن لا يرغبون في أن يصيروا متخصصين أمنيِّين، فيهدف هذا الكتاب إلى تقديم التشفير باعتباره موضوعًا شائقًا ومهمًّا. فأحد أهدافه أن يمكِّن القراء مِن فهم المصطلحات المذكورة في الكتب والأفلام التاريخية العديدة عن التشفير، فضلًا عن إدراك أثر التشفير على تاريخنا وما قد يكون له من الأثر مستقبلًا. كما يهدف الكتاب أيضًا إلى تيسير فهم المشكلات التي تَسبب فيها التوافرُ المتزايد لوسائل التشفير لدى الحكومات وهيئات إنفاذ القانون.

لا يوجد شك في أن محاولة فك الشفرات البسيطة تعزز من فهم المرء لعلم التشفير، بل ويصبح الأمر ممتعًا أيضًا؛ لذلك، على الرغم من أن هذا الكتاب ليس كتابًا دراسيًّا، فإنه يشتمل على عدد من «التمارين»؛ ومن ثَمَّ فإن القارئ مدعوٌّ لفكِّ شفرة بعض الخوارزميات. ويجب ألا يؤدي فشل القارئ في فك الشفرات إلى إثنائه عن استكمال قراءة الكتاب. ومع ذلك يستأهل الأمر على الأرجح محاولة جادة لحلها. وتشتمل هذه التمارين عادةً على عمليات إحلال للحروف، ولا يتطلب حل التمارين اشتراطات معرفية رياضية.

على الرغم من عدم وجود أي اشتراطات معرفية رياضية مسبقة لفهم هذا الكتاب، ليس هناك شك في أن أنظمة التشفير الحديثة تتضمن على نحو دائم إجراء عمليات رياضية. بالإضافة إلى ذلك، تعمل معظم الخوارزميات الحديثة وفق أرقام ثنائية (بِتات) عوضًا عن الأحرف الهجائية. وإقرارًا منا بذلك، أدرجنا ملحقًا قصيرًا بالفصل الثالث يتضمن بعض المفاهيم الرياضية الأساسية. مرة أخرى، فإننا نشجع القراء على محاولة فهم الاصطلاحات الرياضية، لكن يجب أن يطمئنوا إلى عدم حاجتهم الضرورية إلى هذه المفاهيم فيما يلي ذلك من أجزاء الكتاب.

الفصل الثاني

فهم التشفير

(١) مقدمة

في هذا الفصل نقدِّم المصطلحات والمفاهيم الأساسية للتشفير. هدفنا أن يتَّسم عرضنا بشيء من التبسيط، وأن نقدِّم أكبر صورة عامة ممكنة عن الموضوع.

(٢) المصطلحات الأساسية

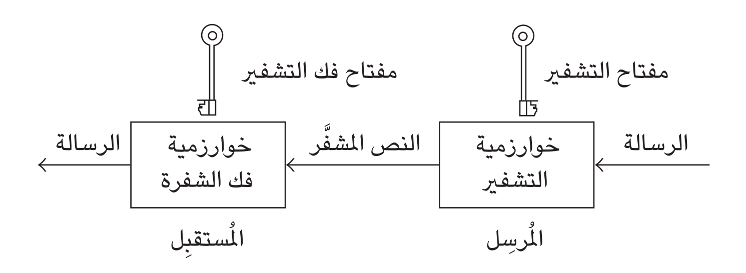
تتمثل فكرة أي نظام تشفير في إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غيرَ مفهوم بالنسبة إلى أي شخص غير مصرَّح له بالاطلاع عليها. يتمثل الاستخدامان الأكثر شيوعًا للتشفير في تخزين البيانات بأمان في ملف كمبيوتر أو نقْلها عبر قناةٍ غير آمنة مثل الإنترنت. في كلتا الحالتين، حقيقةُ كون المستند مشفرًا لا تمنع الأشخاص غير المصرَّح لهم بالوصول إليه، ولكنها تضمن عدم تمكُّنهم من فهم ما يرونه.

غالبًا ما يطلَق على المعلومات المُراد إخفاؤها اسمُ «النص الأصلي»، فيما يطلق على عملية إخفائها اسم «التشفير». ويطلق على النص الأصلي المشفَّر اسم «النص المشفَّر» أو «بيان التشفير»، كما يطلق على مجموعة القواعد المستخدمة في تشفير معلومات النص الأصلي «خوارزمية التشفير». عادةً، تعتمد هذه الخوارزمية على «مفتاح التشفير»؛ وهو يمثل مدخلًا لها بالإضافة إلى الرسالة. وحتى يتمكن المتلقي من استرجاع الرسالة من خلال النص المشفَّر، يجب أن تتوافر «خوارزمية فك التشفير» التي، عند استخدامها مع «مفتاح فك التشفير» المناسب، تسترجع النص الأصلي من النص المشفَّر.

بوجه عام، تعتبر مجموعة القواعد التي تؤلِّف إحدى هذه «الخوارزميات التشفيرية» معقدة للغاية وتحتاج إلى التصميم بعناية. بيْد أنه في إطار أهداف هذا الكتاب، يمكن

للقارئ النظرُ إلى هذه الخوارزميات على أنها «صِيَغ سحرية» تحوِّل البيانات إلى صورة غير مقروءة بمساعدة مفاتيح التشفير.

يبيِّن الشكل التالي وصفًا تخطيطيًّا لاستخدام أحد «أنظمة التشفير» لحماية رسالة منقولة:



يطلق على كلِّ مَن يعترض رسالة خلال انتقالها اسم «مُعترض». هذا، ويستخدم مؤلفون آخرون أسماء أخرى، مثل «متنصِّت»، و«خصم»، و«غريم»، و«شخص سيئ». إلا أنه يجب الإشارة إلى أن المعترضين يمكن أن يكونوا «أشخاصًا طيبين» في بعض الأحيان، وهو ما سوف نتحدث عنه بمزيد من التفصيل لاحقًا. وحتى إن علم المعترضون بخوارزمية فك التشفير، فإنهم في العموم لا يعرفون مفتاح فك التشفير. ومن المأمول أن تَمنع عدم المعرفة هذه المعترضين من معرفة النص الأصلي. وعلم «التشفير» هو علم تصميم أنظمة التشفير، بينما يشير «تحليل النص المشفَّر» إلى العملية التي يجري من خلالها استنباط المعلومات حول النص الأصلي دون معرفة مفتاح التشفير المناسب. أما علم «التعمية» فهو مصطلح جامع يشمل كلًّا من التشفير وتحليل النص المشفر.

من الأهمية بمكان معرفة أن تحليل النص المشفَّر قد لا يكون الوسيلة الوحيدة التي يستطيع بها الطرفُ المعترض الاطلاعَ على النص الأصلي.

هَبْ — على سبيل المثال — أن أحد الأشخاص يخزِّن البيانات المشفَّرة على جهاز الكمبيوتر المحمول؛ بداهةً، يحتاج هذا الشخص إلى طريقةٍ ما لاسترجاع مفتاح فك التشفير لقراءة المعلومات المخزَّنة. إذا تضمن ذلك كتابة هذا المفتاح على ورقة يلصقها على غطاء جهاز الكمبيوتر المحمول، فسيحصل أي شخص يسرق جهاز الكمبيوتر على المفتاح دون حاجة إلى إجراء عملية تحليل للنص المشفَّر. يعتبر هذا المثال نموذجًا بسيطًا يشير إلى الحاجة إلى ما هو أكثر من مجرد استخدام خوارزمية تشفير جيدة لحماية

البيانات. في واقع الأمر، ومثلما نؤكد غير مرة، يعتبر ضمان حماية مفاتيح التشفير أمرًا مهمًّا للغاية لضمان تحقيق الحماية لأنظمة التشفير.

عمليًّا، تتضمن معظمُ هجمات تحليل النص المشفَّر محاولةَ تحديدِ مفتاح فك التشفير. وفي حال نجاح الطرف المعترض، تصبح لديه المعرفة نفسها التي يمتلكها المتلقي المقصود؛ ومن ثَمَّ يستطيع فك شفرة جميع المراسلات الأخرى إلى حين تغيير مفاتيح التشفير. قد تكون هناك حالات لا يعدو فيها الهدف الوحيد للطرف المعترض سوى قراءة رسالة معينة. ومع ذلك عندما يصِف المؤلفان خوارزميةً ما بأنها «مكسورة»، فإنهما يقصدان عادةً بذلك أن الطرف المعترض اكتشف طريقة عملية يستطيع من خلالها تحديد مفتاح فك التشفير.

بطبيعة الحال، لا يستطيع الطرف المعترض فك خوارزمية تشفير إلا إذا توفرت لديه المعلومات الكافية التي تمكنه من معرفة المفتاح الصحيح، أو — على نحو أكثر شيوعًا — تحديد المفاتيح غير الصحيحة. من الأهمية بمكان معرفة أن هذه المعلومات الإضافية تكون على الأرجح في غاية الأهمية بالنسبة إلى الطرف المعترض. هَبْ أن الطرف المعترض يعلم أن النص الأصلي كان باللغة الإنجليزية، وأن عملية فك التشفير لبعض أجزاء النص المشفَّر باستخدام مفتاحٍ جرى تخمينه لا تسفر عن نصٍّ أصلي ذي معنًى في الإنجليزية؛ في هذه الحالة، سيُعد المفتاح الذي جرى تخمينه غير صحيح.

ثمة حقيقة مهمة يجب أن تكون قد اتضحت من خلال هذه المقدمة؛ ألا وهي أن معرفة مفتاح التشفير ليست ضرورية للحصول على الرسالة من خلال النص المشفَّر. تعتبر هذه الملاحظة البسيطة هي أساس ورقة ديفي-هلمان البحثية بَالغة التأثير. فقد كان لها أثر عظيم على علم التشفير الحديث، كما أسفرت عن تقسيم طبيعي بين نوعين من أنظمة التشفير؛ ألا وهما النظام المتناظر والنظام غير المتناظر.

يطلق على نظام التشفير اسم نظام «تقليدي» أو «متناظر» حال سهولة استنباط مفتاح فك التشفير من خلال مفتاح التشفير. في واقع الأمر، غالبًا ما يكون هذان المفتاحان متطابقين بالنسبة إلى أنظمة التشفير المتناظرة. لذلك، يُطلق على هذه الأنظمة عادةً اسم أنظمة «المفتاح السري» أو «المفتاح الواحد». في المقابل، إذا لم يكن ممكنًا من الناحية العملية استنباط مفتاح فك التشفير من خلال مفتاح التشفير، فإن نظام التشفير يسمى «غير متناظر» أو «ذا مفتاح معلن». ثمة سبب يجب أن نَعِيَهُ تمامًا وراء التمييز بين هذين النوعين من الأنظمة؛ فلمنع أي معترض لديه معرفة بالخوارزمية من الحصول

على النص الأصلي عن طريق نص مشفَّر جرى اعتراضه، من الضروري الاحتفاظ بسرية مفتاح فك التشفير. وفي حين أنه في حالة النظام المتناظر، يتطلب الأمر الاحتفاظ بسرية مفتاح التشفير أيضًا، فإنه في حالة النظام غير المتناظر، تكون معرفة هذا المفتاح غير ذات فائدة عملية للطرف المعترض. في الواقع، يمكن الإعلان عن هذا المفتاح، وعادة ما يحدث ذلك. يترتب على ذلك غياب حاجة المُرسِل والمستقبِل للنص المشفر لتبادل أي أسرار بينهما. في الواقع، ربما لا توجد حاجة في أن يثق أحدهما في الآخر.

على الرغم من أن العبارات في الفقرة السابقة قد تبدو بسيطة وبديهية، فإن النتائج المترتبة عليها بعيدة الأثر. يفترض الرسم الموضح سابقًا حصول المُرسِل والمستقبِل على «زوج متطابق» من المفاتيح. في واقع الأمر، ربما يكون من الصعوبة بمكان بلوغهما هذا الوضع. على سبيل المثال، في حالِ كان نظام التشفير متناظرًا ربما كانت هناك حاجة إلى توزيع قيمة المفتاح السري قبل تبادل الرسائل السرية. ويجب عدم الاستهانة بمشكلة توفير الحماية المناسبة لهذه المفاتيح. في واقع الأمر، تعتبر مشكلة إدارة المفاتيح بوجهٍ عام — والتي تشمل إنشاءها وتوزيعها وتخزينها وتغييرها وتدميرها — أصعبَ جوانب الحصول على نظام آمن. وعادة ما تختلف المشكلات المصاحبة لمشكلة إدارة المفاتيح باختلاف نظام التشفير بين متناظر وغير متناظر. فكما رأينا، إذا كان نظام التشفير متناظرًا، ربما ظهرت الحاجة إلى توافر القدرة على توزيع المفاتيح مع الاحتفاظ بسرية قِيَمها. أمَّا في حال نظام التشفير غير المتماثل، فيمكن التغلب على هذه المشكلة من خلال توزيع مفاتيح التشفير فقط التي لا حاجة إلى جعلها سرية. ومع ذلك تظهر مشكلة أخرى تتمثل في ضمان التحقق من مفتاح تشفير كل مشارك؛ أيْ ضمان معرفة الشخص المستخدم لقيمة مفتاح التشفير المعلن لهوية «مالك» مفتاح فك التشفير المقابل له.

عندما عرضنا الفرق بين أنظمة التشفير المتناظرة وغير المتناظرة، كنا نفترض معرفة الطرف المعترض بالخوارزمية. بطبيعة الحال، لا يكون ذلك صحيحًا دومًا. ومع ذلك ربما كان من الأفضل بالنسبة إلى مصمِّم نظام التشفير أن يفترض امتلاك المُعترِض المحتمِل لأكبر قدر ممكن من المعرفة والمعلومات الاستخباراتية العامة قدر الإمكان. هناك مبدأ مشهور في علم التشفير يقول إنَّ أمْن أي نظام تشفير يجب ألا يعتمد على الاحتفاظ بسرية خوارزمية التشفير؛ وهو ما يجعل سلامة النظام يعتمد تبعًا لذلك على الاحتفاظ بسرية مفتاح فك التشفير وحسب.

يتمثل أحد أهداف دراسة علم التشفير في تمكين أي شخص يرغب في تصميم أو تنفيذ نظام تشفير من تقييم ما إذا كان ذلك النظام آمنًا بما يكفي لتحقيق الغرض من

تنفيذه. ولتقييم مدى أمان نظام التشفير نضع الافتراضات الثلاثة التالية، والتي نُطلق عليها «ظروف أسوأ الحالات»:

ظرف أسوأ الحالات ١: يمتلك الطرف الذي يتولى عملية تحليل النص المشفر معرفة كاملة بنظام التشفير.

ظرف أسوأ الحالات ٢: يحصل الطرف الذي يتولى عملية تحليل النص المشفر على قدر كبير من هذا النص.

ظرف أسوأ الحالات ٣: الطرف الذي يتولى عملية تحليل النص المشفر يعرف النص الأصلي المكافئ لقدرٍ محدد من النص المشفَّر.

في أيٍّ من هذه الحالات، يجب محاولة تحديد ما تعنيه ألفاظُ «قدر كبير» و«قدر محدد» بواقعية، وهذا يعتمد على نظام التشفير موضع الاعتبار.

يشير ظرف أسوأ الحالات ١ ضمنًا إلى أننا نؤمن بضرورة عدم الاعتماد على الاحتفاظ بسرية تفاصيل نظام التشفير. لكن هذا لا يعني أنْ نُتيح نظام التشفير للجميع. بطبيعة الحال، ستُعد مهمة الطرف المعترض أكثر صعوبة في حال عدم معرفة نظام التشفير المستخدم، وهو ما يمكن إخفاؤه بدرجة ما حاليًّا. على سبيل المثال، بالنسبة إلى الأنظمة الإلكترونية الحديثة، يمكن إخفاء خوارزمية التشفير في الأجهزة ذاتها عن طريق استخدام المكونات الإلكترونية متناهية الصغر؛ إذ يمكن إخفاء الخوارزمية بأكملها داخل «شريحة» صغيرة. وللحصول على الخوارزمية يجب على الطرف المعترض «فتح» إحدى هذه الشرائح، وهي عملية دقيقة وتستغرق على الأرجح وقتًا طويلًا للغاية، وإن كان من الممكن تنفيذها؛ إذ يجب ألا نفترض غياب قدرة وقلة صبر الطرف المعترض للقيام بذلك. بالمثل، من الممكن إخفاء أي جزء من الخوارزمية التي جرى تضمينها كبرنامج في الماكينة من خلال برنامج مكتوب بعناية. نؤكد مرة أخرى، ربما يمكن من خلال الصبر وتوفر المهارة الكشفُ عن هذا، بل ربما تصبح الخوارزمية بعينها متاحة للطرف المعترض في بعض الحالات. من وجهة نظر أي مُصنِّع أو مصمم لنظام تشفير، يعتبر ظرف أسوأ الحالات ١ افتراضًا أساسيًّا؛ حيث إن افتراضًا كذلك يُزيل قدرًا كبيرًا من المسئولية النهائية الملقاة على عاتقهم فيما يتعلق بالاحتفاظ بسرية أي نظام تشفير.

يعتبر ظرف أسوأ الحالات ٢ افتراضًا معقولًا. فإذا لم يكن ثمة احتمال لوقوع عملية اعتراض، فلن توجد حاجة إلى استخدام نظام تشفير. ومع ذلك إذا كان الاعتراض

محتملًا، فمن المفترض ألا تتمكن الأطراف المتواصلة إذن من تحديد وقت وقوع عمليات الاعتراض على وجه الدقة؛ ومن ثَمَّ يصير الخيار الأكثر سلامة هو افتراض إمكانية اعتراض جميع المراسلات.

يعتبر ظرف أسوأ الحالات ٣ افتراضًا واقعيًّا أيضًا. فربما يتمكن الطرف المعترض من الحصول على مثل هذا النوع من المعلومات من خلال متابعة انتقال الرسائل وإجراء تخمينات ذكية. بل ربما يتمكن الطرف المعترض أيضًا من اختيار النص الأصلي الذي يعرف النص المشفَّر له. من الأمثلة «الكلاسيكية» التاريخية على ذلك ما وقع خلال الحرب العالمية الثانية عندما جرى تعريض عوَّامة خفيفة لهجوم تفجيري فقط لضمان ظهور الكلمة الألمانية Leuchttonne في رسائل نصوص أصلية كان سيجري تشفيرها باستخدام ماكينات إنيجما للتشفير (انظر كتاب «الحرب السرية» للمؤلف بي جونسون الذي نشرته هيئة الإذاعة البريطانية).

يطلق على عملية الاعتراض التي تستفيد من وجود زوج من نص أصلي ونص مشفَّر معروفين «عملية اعتراض لنص أصلي معروف». إذا انتقى الطرف المعترض النص الأصلي، مثلما كان الحال مع مثال تفجير العوامات الخفيفة المذكور أعلاه، يُطلق على عملية الاعتراض هذه «عملية اعتراض مُنتقاة لنص أصلي». وأخيرًا، يطلق على عملية الاعتراض التي تتضمن معرفة مباشرة من الطرف المعترض للنص المشفَّر فقط «عملية اعتراض نص مشفَّر فقط».

يترتب على قبول ظروف أسوأ الحالات هذه افتراضُ أن المعلومات الوحيدة التي تميِّز بين المتلقي الحقيقي للمراسلات والطرف المعترض تتمثل في معرفة مفتاح فك التشفير. من هنا، يعتمد توافر الأمن في نظام التشفير كلية على سرية مفتاح فك التشفير، وهو ما يعزز ما أكدنا عليه سابقًا من أهمية توفر إدارة جيدة لمفاتيح نظام التشفير.

يجب أن نؤكد على أن تقييم مستوى الأمان في أي نظام تشفير ليس علمًا بالمعنى الدقيق؛ إذ تقوم جميع عمليات التقييم على وضع الافتراضات، لا من خلال المعرفة المتوفرة للطرف المعترض فحسب، بل أيضًا من خلال الأدوات والموارد المتوفرة له. ودونما شك، يتمثل المبدأ العام الأفضل على الإطلاق في افتراض الأسوأ وتحري الحرص، حتى لو كان هذا الحرص مبالغًا فيه. من الأهمية بمكان أيضًا التأكيد على أن السؤال المناسب عمومًا في هذا المقام ليس: «هل هذا النظام آمن تمامًا؟» وإنما: «هل هذا النظام آمن بما يكفي لتنفيذ الغرض من تطبيقه؟» وتعتبر الملاحظة الأخيرة في غاية الأهمية، كما يجب

الاعتراف بوجود ضرورات لتوفير الأمن غير المكلف ومنخفض المستوى في بعض الحالات. بالنسبة إلى معظم التطبيقات غير العسكرية، يدخل توفير الأمن في أنظمة التشفير في باب المصروفات العامة التي يجب وجود تبرير لها من المنظور التجاري. بالإضافة إلى ذلك، قد تكون إضافة أدوات توفير الحماية الأمنية ذات تكلفة مرتفعة؛ وهو ما قد يؤدي إلى الحد من كفاءة الأداء العام لنظام التشفير. من هنا، توجد حاجة طبيعية للإبقاء على الحالة الأمنية عند حدها الأدنى. وتتمثل إحدى الطرق الشائعة في تحديد مستوى الأمن المطلوب توفره في وضع تقديرات بالوقت اللازم لحماية المعلومات. إذا أطلقنا على ذلك «وقت التغطية» المطلوب للنظام، فسيتوفر لدينا مؤشر عام لمستوى الأمن المطلوب توفره في نظام التشفير. على سبيل المثال، ربما يعتبر نظامُ التشفير المناسب لشبكة تكتيكية مؤقتة، لا يتجاوز وقت تغطية المعلومات المتناقلة عبرها بضع دقائق، «أضعفَ» كثيرًا من نظام التشفير المطلوب في نظام استراتيجي قد يصل وقت تغطية المعلومات فيه إلى عقود، مثلما هو الحال مع الأسرار الحكومية والسجلَّات الطبية.

إذا افترضنا عدم سرية خوارزمية فك التشفير، فسيكون هناك أسلوب واحد بديهي يجري استخدامه في الاعتراض؛ فقد يحاول المعترضون، على الأقل من الناحية النظرية، تخمين كل مفتاح فك تشفير ممكن فيما «يأملون» في تحديد المفتاح الصحيح. يطلق على عملية الاعتراض هذه «بحث شامل عن المفتاح» أو — بعبارة أخرى — «عملية اعتراض باستخدام القوة المفرطة». وبطبيعة الحال، لا يمكن أن تنجح عملية اعتراض كهذه إلا إذا كان لدى الطرف المعترض طريقة ما للتعرف على المفتاح الصحيح أو — مثلما هو أكثر شيوعًا — إذا كان الطرف المعترض يستطيع استبعاد المفاتيح غير الصحيحة. على سبيل المثال، في حال وجود عملية اعتراض لنص أصلي معروف، سيصبح من البديهي ألا يمثِّل أيُّ مفتاح فك تشفير لا يسفر عن الحصول على النص الأصلي الصحيح المقابل للنص المشفَّر بكامله؛ المفتاحَ الصحيح. لكن، مثلما نرى عندما نأخذ بعين الاعتبار بعضَ الأمثلة البسيطة، ما لم يكن هناك قدر مناسب من أزواج النص الأصلي والنص المشفَّر المقابل له، ربما سيكون هناك العديد من الخيارات غير الصحيحة لمفتاح فك التشفير التي تعطي الإجابات الصحيحة لكامل النص المشفر المتاح. وفي حالٍ ما إذا كانت لغة المراسلات تتسم بالتراكيب اللغوية النمطية، فعندئذٍ يمكن استخدام أسلوب الإحصاءات اللغوية لاستبعاد بعض المفاتيح.

بلغْنا الآن مرحلة نستطيع من خلالها البدء في بيان بعض المعايير الأساسية لتقييم مدى ملاءمة نظام تشفير معين لتطبيق بعينه. يحدد مستخدمو النظام وقت التغطية.

ويجب على مصممي النظام معرفة عدد مفاتيح فك التشفير. وإذا وضع المصممون افتراضات حول مدى سرعة الطرف المعترض في تجربة كل مفتاح، فإنهم سيستطيعون وضع تقديرات بالوقت المتوقع الذي تستغرقه عملية بحث شاملة عن المفتاح للكشف عنه. وإذا كان هذا الوقت المُقدَّر أقصر من وقت التغطية، فسيكون النظام في غاية الهشاشة. من هنا، يتمثل الاشتراط الأساسي في وضع نظام تشفير في ضرورة أن يكون الوقت المقدَّر اللازم للتوصل إلى مفتاح صحيح من خلال عملية بحث شاملة أطول كثيرًا من وقت التغطية.

عندما ميَّزنا بين الخوارزميات المتناظرة وغير المتناظرة، تحدثنا عن الحاجة إلى توفر الثقة بين المرسل والمستقبل. ولقرون طويلة، قبل نشر ورقة ديفي-هلمان البحثية الشهيرة، كان يفترض أن الرسائل المشفرة لا يجري تبادلها إلا بين أطراف تتوفر الثقة بينها. كان مفهوم القدرة على إرسال رسائل إلى طرف لا تتوفر الثقة فيه مسألة مستحيلة. سوف نناقش خوارزميات المفاتيح المعلنة في الفصول التالية، لكننا نذكر هنا مثالًا معروفًا على كيف أنه من الممكن ضمان تسليم هدية إلى متلقيها المقصود بأمان، على الرغم من مرورها عبر أيدي أطراف كثيرة مناوئة ربما ترغب في الاستيلاء عليها.

في هذا المثال سنفترض أن ثمة مرسِلًا لديه هدية، وأنه يرغب في حفظها في حقيبة محكَمة الغلق بقفل ويريد إرسالها إلى أحد الأشخاص، الذي هو على غير استعداد لأنْ يأتمنه على مفتاحه. بدلًا من ذلك، يبلغ المُرسلُ المستقبلَ المقصود برغبته في بيع قفله والمفتاح. نفترض عدم وجود أي شخص آخر يستطيع العثور على مفتاح يمكنه من فض مغاليق أقفال المرسل أو المستقبل وأن الأقفال والحقيبة في حالة جيدة لا تسمح بفتحها عنوة للحصول على الهدية. يتخذ المرسل والمستقبل كلاهما الخطوات التالية لضمان تسليم الهدية:

خطوة ١: يضع المرسل الهدية داخل الحقيبة التي يحكم إغلاقها بواسطة القفل، وينزع المفتاح، ثم يرسل الحقيبة المغلقة إلى المستقبل.

ملاحظة: بينما الحقيبة في طريقها من المرسل إلى المستقبل، تتمتع الحقيبة بالحماية اللازمة من جميع الأطراف المناوئة؛ نظرًا لعدم قدرة هذه الأطراف على نزع قفل الحقيبة. لكن المستقبِل لا يستطيع هو الآخر الحصول على الهدية.

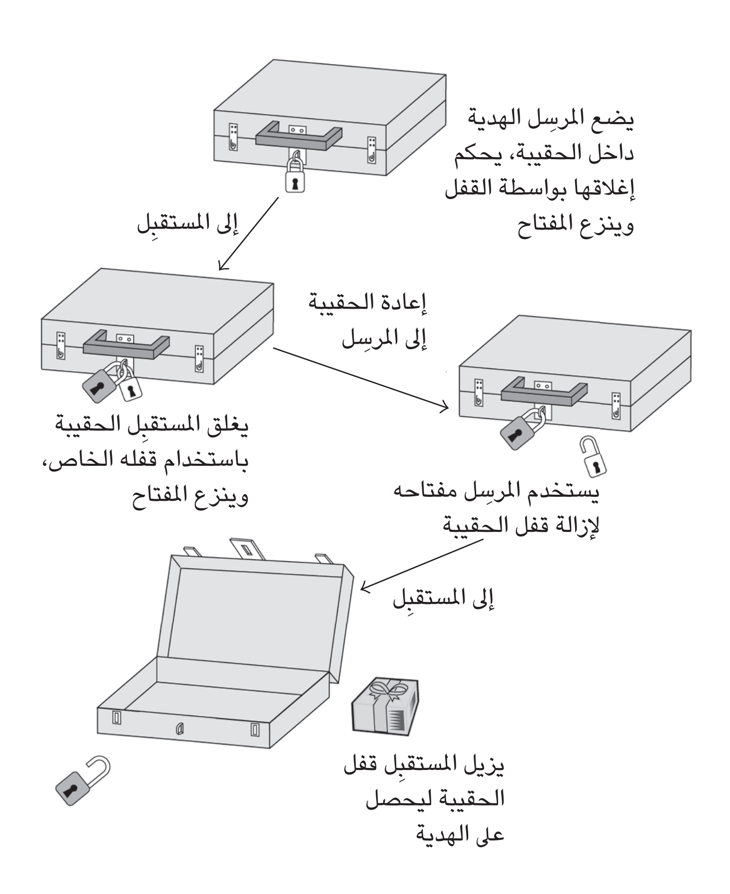
خطوة ٢: يغلق المستقبِل الحقيبة باستخدام قفله الخاص، وينزع المفتاح، ثم يعيد الحقيبة إلى المرسل.

ملاحظة: يوجد قفلان الآن في الحقيبة؛ وهو ما لا يجعل أحدًا يحصل على الهدية التي بداخلها.

خطوة ٣: يستخدم المرسِل مفتاحه لإزالة قفله من الحقيبة ثم يعيدها إلى المستقبِل.

ملاحظة: لا يوجد سوى قفل المستقبِل في الحقيبة.

خطوة ٤: يزيل المستقبل قفل الحقيبة الخاص به ليحصل على الهدية.



تتمثل النتيجة النهائية لهذه السلسلة من الأحداث في أن الهدية جرى إرسالها إلى المستقبل دون أن يكشف أيٌّ من المرسل أو المستقبل عن مفتاحيهما السريين. إنهما لم يكونا في حاجةٍ إلى وثوق أحدهما في الآخر. بطبيعة الحال، من المستبعد للغاية أن تكون افتراضاتنا بشأن المفاتيح وقوة الأقفال واقعية، لكن عندما نناقش تشفير المفاتيح المعلنة يُستعاض بالمعادلات الرياضية، التي تُعد أكثر قبولًا، عن هذه الافتراضات. تتمثل النقطة الرئيسية فيما بيَّنَّاه، على الأقل من الناحية النظرية، في أن مفهوم توفير اتصالات آمنة دون وجود ثقة متبادلة ربما يكون مسألة ممكنة.

في هذا المثال المبسَّط، يجب أن نقرَّ بأن المرسل لا يملك سبيلًا لمعرفة أيُّ الأقفال موجود في الحقيبة، وأنه من المحتمل أن ينتحل أحدُ الغرماء شخصيةَ الطرف المستقبِل ويضع قفله الخاص على الحقيبة. هذه مشكلة تحتاج إلى حل. يشبه سؤال «من صاحب هذا القفل؟» في هذا المثال سؤال «من صاحب هذا المفتاح المعلن؟» الذي يعتبر سؤالًا مهمًّا عند استخدام أنظمة تعتمد على مفاتيح التشفير المعلنة.

قبل أن نتوغل أكثر من هذا في الجانب النظري، سنذكر بعض الأمثلة التاريخية في الفصل التالي لتوضيح النظرية وللتأكد من استيعاب التعريفات.

الفصل الثالث

الخوارزميات التاريخية: أمثلة بسيطة

(١) مقدمة

في هذا الفصل نقدِّم بعض الأمثلة «البدائية» لتوضيح الأفكار الأساسية التي تناولناها في الفصل الثاني. نضرب هذه الأمثلة أيضًا لإلقاء بعض الضوء على نوع الهجمات التي قد تشنها الأطراف المعترضة، ولبيان بعض الصعوبات التي يواجهها مصممو الخوارزميات. تنتمي جميع أمثلة الخوارزميات المذكورة هنا إلى النوع المتناظر، وهي أمثلة لخوارزميات جرى تصميمها واستخدامها قبل وقت طويل من اقتراح نظم التشفير ذات المفتاح المعلن. ويستهدف هذا الفصل القارئ غير المتخصص في العلوم الرياضية، لكن توجد أمثلة نشعر فيها بالحاجة إلى طرح المبادئ الرياضية الأساسية فيها، خاصة علم المقياس الحسابي. عندما يحدث هذا، لن يتأثر استيعاب القارئ جراء تجاوزه الجانب الحسابي في الأمثلة المذكورة. ومع ذلك سوف نطرح أمثلة رياضية توضيحية مبسطة (في الملحق الوارد في نهاية الفصل) لتمكين جميع القراء من فهم النص إذا رغبوا في ذلك.

تعتبر أمثلة الخوارزميات هذه قديمة ولا تعبر في واقع الأمر عن أيٍّ مِن أساليب التشفير الحديثة. ومع ذلك من الأهمية بمكان دراسةُ عدد من الأنظمة البدائية كان يجري التشفير فيها من خلال استبدال الأحرف بعضها ببعض، فيما يُطلق عليه استبدال الأحرف، و/أو تغيير ترتيب الأحرف. يوجد عدد من الأسباب وراء ذكر مثل هذه الأمثلة؛ أوَّلها: تمكِّننا هذه الأنظمة من ضرب أمثلة بسيطة وسهلة الاستيعاب تبين المفاهيم الأساسية، كما تمكِّننا من بيان عدد من نقاط الضعف في الشفرات. كما يوجد سبب آخر

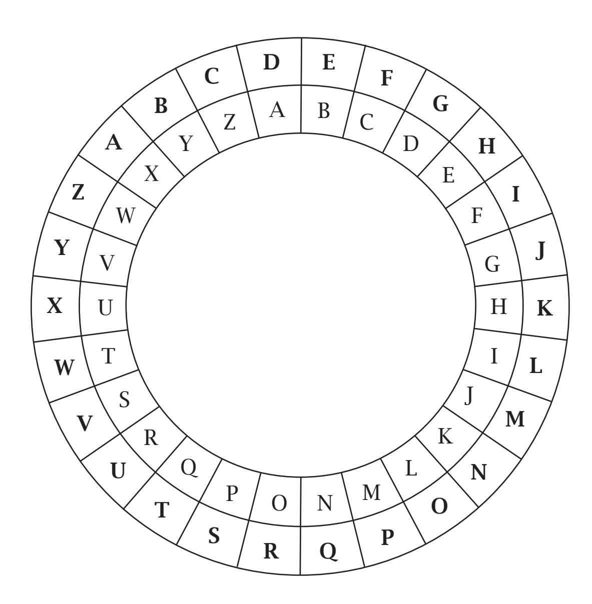
يتمثَّل في كونها أمثلةً تقدِّم متعة بالغة في حلها، وبما أنها لا تتضمن في الأغلب الكثيرَ من العمليات الرياضية، يستطيع «الهواة» ممن لم يتلقَّوا تدريبًا علميًّا الاستمتاع بها.

(٢) شفرة قيصر

كانت «شفرة قيصر»، التي ذكرها يوليوس قيصر في كتابه «الحروب الغاليَّة»، من أوائل الأمثلة على استخدام الشفرات. وفق هذه الشفرة، يجري تشفير الأحرف من A إلى W من خلال تمثيل كلٍّ مِنها بالحرف الثالث بعده في ترتيب الأبجدية. بينما يجري تمثيل الأحرف X، وY، وZ بالأحرف **A**، و**B**، و**C** على الترتيب. وعلى الرغم من استخدام قيصر «عملية إزاحة» تتألف من ثلاثة أحرف، كان يمكن تصميم شفرة مشابهة من خلال استخدام أي عدد من 1 إلى 25. في واقع الأمر، يُنظَر إلى أي عملية إزاحة في نظام التشفير بوصفها مثالًا لشفرة قيصر.

مرة أخرى نستخدم رسمًا توضيحيًّا لبيان إحدى شفرات قيصر؛ يمثِّل الشكل الموضح حلقتين تتمحوران حول مركز واحد؛ حيث تمتلك الحلقة الخارجية منهما حرية الدوران. إذا بدأنا بالحرف **A** في الحلقة الخارجية حول حرف A في الحلقة الداخلية، فإن الإزاحة بمقدار 2 ستؤدي إلى وجود حرف **C** قبالة الحرف A وهكذا. هناك، إذن، 26 وضع ضبط بما في ذلك إزاحة مقدارها صفر (التي هي بطبيعة الحال نفس الإزاحة التي مقدارها 26). ويحدد عدد حركات الإزاحة مفتاح التشفير ومفتاح فك التشفير في شفرة قيصر.

بمجرد الموافقة على عدد حركات الإزاحة، تتحقق عملية التشفير في شفرة قيصر من خلال النظر إلى كل حرف من حروف النص الأصلي على أنه بمنزلة حلقة داخلية والاستعاضة عنه بالحرف الذي يقع قبالته في الشكل الموضح. وفي عملية فك التشفير، نُجري العملية العكسية. من هنا، وفق الشكل المبين، يتمثل النص المشفر لرسالة النص الأصلي DOG في **GRJ** عند الإزاحة بمقدار 3 حركات، بينما يكون CAT هو النصَّ الأصلي المكافئ للنص المشفر **FDW**. من أجل منح القارئ مزيدًا من الثقة في فهم نظام شفرة قيصر نطرح أربع عبارات للتأكد. إذا كان عدد حركات الإزاحة 7، فسيكون نص التشفير المناظر للنص الأصلي VERY هو **CLYF**، بينما يكون النص الأصلي SUN، عند الإزاحة 17 حركة، هو النصَّ المناظر للنص المشفَّر **JLE**.



«ماكينة» تنفِّذ شفرة قيصر.

في عرضنا لشفرة قيصر، يكون كلٌّ من مفتاح التشفير ومفتاح فك التشفير مساويًا لعدد حركات الإزاحة بينما تختلف قواعد التشفير وفك التشفير. ومع ذلك كان بإمكاننا تغيير الصياغة قليلًا بحيث تتطابق القاعدتان بينما تختلفان في مفاتيح التشفير وفك التشفير. نرى ذلك مثلًا عند الإزاحة بمقدار صفر أو 26 حيث يتحقق الأثر نفسه، وعند الإزاحة بعدد حركات يتراوح بين صفر و25 يكون التشفير مع هذا العدد من حركات الإزاحة مكافئًا لفك التشفير مع عدد حركات الإزاحة الجديد الذي يجري الحصول عليه من خلال طرح عدد حركات الإزاحة الأصلي من 26. لذا — على سبيل المثال — يكون التشفير عند الإزاحة بمقدار 8 حركات مكافئًا لفك التشفير عند الإزاحة بعدد حركات $26 - 8 = 18$. يمكِّننا ذلك من استخدام القاعدة نفسها في عمليتَيِ التشفير وفك التشفير من خلال إجراء عملية فك تشفير بالإزاحة 18 حركة تكافئ التشفير بالإزاحة 8 حركات.

ذكرنا سابقًا عمليات البحث الشاملة المرهقة عن المفاتيح، ومن البديهي أنه بما أن هناك 26 حرفًا فقط لا غير، يعتبر نظام شفرة قيصر عرضة لمثل هذا النمط من

الهجمات. قبل أن نضرب مثلًا على كيفية تحقيق ذلك، يجب الإشارة إلى أحد مواطن الضعف الأخرى لهذا النظام: يمكن تحديد المفتاح من خلال معرفة زوج واحد من حروف النص الأصلي والنص المشفر المقابل له، وهو ما يُعد قدرًا ضئيلًا للغاية من المعلومات.

أسهل طريقة لتوضيح عملية البحث الشاملة عن المفتاح هي عرض مثال كامل وسهل — بما أنه يوجد 26 مفتاحًا فقط — لنظام شفرة قيصر. لنفترض أننا نعرف أن نظام شفرة قيصر يجري استخدامه، وأننا نتوقع رسالة باللغة الإنجليزية، وأننا نجحنا في اعتراض النص المشفَّر **XMZVH**. إذا كان المرسل أجرى 25 حركة إزاحة لتنفيذ عملية التشفير فستُجرى عملية فك التشفير إذن من خلال إجراء حركة إزاحة واحدة؛ بحيث يكون YNAWI هو نص للرسالة. وبما أن تلك الرسالة لا معنًى لها في اللغة الإنجليزية، يمكننا أن نستبعد باطمئنانٍ العدد 25 كقيمة لعدد حركات الإزاحة. يبيِّن جدول ٣-١ نتيجة محاولات الانتقال بصورة منهجية بعدد حركات إزاحة من 25 إلى 1 بترتيب تنازلي.

لا توجد كلمة إنجليزية واحدة في جدول ٣-١ ذات معنًى سوى كلمة CREAM؛ ومن ثَمَّ، يمكن أن نستنبط من ذلك أن مفتاح التشفير هو 21، وهو ما يمكننا من فك شفرة جميع الرسائل المستقبلية إلى حين تغيير المفتاح. وعلى الرغم من النجاح الكامل لعملية البحث الشاملة هذه عن المفتاح، من الأهمية بمكان إدراك أنه في حالة الشفرات الأكثر تعقيدًا قد لا يمكن تحديد المفتاح على وجه الدقة من خلال عملية بحث شاملة واحدة فقط؛ كل ما هنالك أنه، على الأرجح، سيَحِد من عدد الاحتمالات من خلال استبعاد الاحتمالات غير الواردة تمامًا. مثال على ذلك، وبالعودة إلى شفرة قيصر، نلاحظ أن إجراء عملية بحث شاملة عن مفتاح التشفير للنص المشفَّر **HSPPW** يؤدي إلى احتمالين تتولد عنهما كلمتان إنجليزيتان ذواتا معنًى للرسالة المفترضة. (يتمثل الاحتمالان في احتمال حركات إزاحة عددها 4، تكشف عن كلمة DOLLS، واحتمال حركات إزاحة عددها 11، تكشف عن كلمة WHEEL.)

عندما يحدث ذلك نحتاج إلى توفُّر المزيد من المعلومات، ربما سياق الرسالة المفترضة أو المزيد من نص التشفير، قبل أن نتمكن من تحديد المفتاح على وجه الدقة. وعلى الرغم من ذلك، تشير نتيجة البحث الشاملة عن المفتاح أننا قللنا من عدد احتمالات المفاتيح كثيرًا، وأننا إذا اعترضنا المزيد من النص المشفَّر، فلن نحتاج إلى إجراء عملية بحث شاملة

جدول ٣-١: مثال على عملية بحث شامل عن المفتاح: نص مشفَّر **XMZVH**.

مفتاح التشفير	«الرسالة» المفترضة	مفتاح التشفير	«الرسالة» المفترضة	مفتاح التشفير	«الرسالة» المفترضة
0	XMZVH	17	GVIEQ	8	PERNZ
25	YNAWI	16	HWJFR	7	QFSOA
24	ZOBXJ	15	IXKGS	6	RGTPB
23	APCYK	14	JYLHT	5	SHUQC
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	12	LANJV	3	UJWSE
20	DSFBN	11	MBOKW	2	VKXTF
19	ETGCO	10	NCPLX	1	WLYUG
18	FUHDP	9	ODQMY		

أخرى. في حقيقة الأمر، في حالة هذا المثال البسيط، لن نحتاج إلا لتجريب قيمتين فقط لعدد حركات الإزاحة؛ وهما 4 و11.

ثمة ملاحظة أخرى مثيرة للاهتمام في هذا المثال. فخلال حله، سيكتشف القارئ كلمتين إنجليزيتين تتألفان من خمسة أحرف؛ بحيث يجري الحصول على واحدة من خلال الأخرى باستخدام شفرة قيصر عن طريق إجراء عدد 7 حركات إزاحة. ربما ترغب في أن تمضي في إجراء ذلك وأن تحاول العثور على أزواج من كلمات أطول، بل وربما عبارات ذات معنًى، تكون كلٌّ منها ناتجة عن حركات إزاحة للأخرى.

يتبين من هذا المثال البسيط سهولة كسر شفرات قيصر. ومع ذلك نجح يوليوس قيصر في استخدامها؛ ربما لأن أعداءه لم يجُلْ بخاطرهم استخدامه أيَّ شفرات. حاليًّا، لا يوجد أحد ليس على دراية بالتشفير.

يمكن استخدام مصطلحات رياضية لتحل محل عجلة قيصر لوصف شفرة قيصر. سنذكرها هنا، لكن لا ضرر في أن يتخطى هذا الجزء مَن لا يألف استخدام المصطلحات الرياضية وينتقل إلى الجزء التالي.

عندما بدأنا الحديث عن شفرة قيصر ذكرنا أن إجراء 26 حركة إزاحة يساوي إجراء صفر حركة إزاحة؛ وذلك لأن إجراء 26 حركة إزاحة هو بمنزلة دورة كاملة لعجلة قيصر. بالمثل، يمكن تطبيق هذا المنطق لبيان أن إجراء أي عدد من الحركات يكافئ حركة إزاحة بين قيمتَيْ صفر و25. على سبيل المثال، تتأتى 37 حركة إزاحة من خلال إجراء دورة كاملة لعجلة قيصر ثم الإزاحة 11 حركة. بعبارة أخرى، بدلًا من القول بأن 37 حركة إزاحة تكافئ 11 حركة إزاحة، نكتب 11 = 37 (مقياس 26).

يُعرف هذا باسم استخدام «المقياس الحسابي 26»؛ حيث الرقم 26 هو «المقياس». يلعب المقياس الحسابي، بالنسبة لكثير من المقاييس الأخرى فضلًا عن المقياس 26، دورًا جوهريًّا في عدة مجالات في التشفير. بناءً عليه، نذيِّل هذا الفصل بملحق لتعريف القارئ بالمفاهيم والنتائج ذات الصلة في هذا الفرع من نظرية الأعداد الأساسية.

يُشار في بعض الأحيان إلى شفرات قيصر بأنها «شفرات جمعية». حتى نعرف سبب ذلك، سنخصص قيم أعداد صحيحة للأحرف على النحو التالي:

$$A = 0,\ B = 1,\ \ldots,\ Z = 25$$

يتحقق التشفير باستخدام شفرة قيصر إذن مع الانتقال بعدد حركات إزاحة y من خلال الاستعاضة عن الرقم x بـ x + y (مقياس 26). من هنا على سبيل المثال، بما أن N هو الحرف الرابع عشر من حروف الأبجدية، إذن N = 13. إذا أردنا تشفير N بإجراء 15 حركة إزاحة، نحصل على x = 13 وy = 15؛ وهو ما يعني أن النسخة المشفَّرة من N هي 2 = 28 = 15 + 13 (مقياس 26). وهكذا، شُفِّرت N إلى **C**.

مثلما رأينا، يعتبر عدد المفاتيح بالنسبة إلى الشفرات الجمعية صغيرًا للغاية. إذا حاولنا التفكير في طرق للحصول على نظام شفرات يتضمن عددًا أكبر من المفاتيح، فربما نستخدم عملية الضرب كبديل لقاعدة التشفير في شفرة قيصر. ومع ذلك إذا حاولنا تطبيق قاعدة الضرب هذه، بما أن التشفير يجب أن يكون عملية قابلة للعكس، توجد قيود على عدد «المفاتيح الخاضعة لقاعدة الضرب».

هب أننا نحاول تشفير الرسائل عن طريق ضرب قيم أحرف الرسالة في 2 واستخدام المقياس 26؛ عند إجراء ذلك، يشفَّر كلٌّ مِن A وN إلى **A**، بينما يشفَّر كلٌّ مِن B وO إلى **C** وهكذا. يتبين من ذلك أن الأحرف التي تمثِّلها أعداد زوجية فقط تظهر في أي نص مشفَّر، وأن أي حرف في هذا النص المشفَّر قد يمثِّل حرفًا واحدًا فقط من حرفين،

وهو ما يجعل عملية فك التشفير مستحيلة عمليًّا؛ ومن ثَمَّ لا يمكن الضرب في 2 لإجراء عملية التشفير. يوجد مثال آخر أكثر إثارة وذلك بمحاولة الضرب في 13. في هذه الحالة، سيجري تشفير نصف عدد الأحرف الهجائية إلى **A**، فيما يجري تشفير النصف الآخر إلى **N**. حقيقةً، لا يمكن استخدام سوى أعداد 1، 3، 5، 7، 9، 11، 15، 17، 19، 21، 23، 25 عند الضرب لإجراء عملية التشفير.

(٣) شفرات الاستبدال البسيط

على الرغم من أن توافر عدد كبير من المفاتيح يعتبر شرطًا ضروريًّا لتحقيق الأمن في عملية التشفير، فمن الأهمية بمكان الإشارة إلى أن توفر عدد كبير من المفاتيح لا يضمن بالضرورة قوة نظام التشفير. من الأمثلة على ذلك شفرة الاستبدال البسيط (أو الشفرة أحادية الأحرف) التي نعرضها تفصيلًا هنا. لا يبين عرض هذه الشفرة في هذا الفصل مخاطر الاعتماد على عدد كبير من المفاتيح كمؤشر على قوة الشفرة، بل يبين أيضًا كيف يمكن استغلال الإحصاءات اللغوية، في هذه الحالة الإنجليزية، من قِبَل الطرف المُعترِض.

في حالة شفرات الاستبدال البسيط نكتب الأحرف الأبجدية عشوائيًّا تحت أحرف الهجاء تمامًا كما هي مرتبة أبجديًّا، مثلما هو موضح هنا:

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

تتساوى مفاتيح التشفير وفك التشفير؛ إذ تتمثل في ترتيب الأحرف المكتوبة بخط عريض. تتمثل قاعدة التشفير في «تبديل كل حرف بالحرف الذي يقع تحته» فيما تتمثل قاعدة فك التشفير في تنفيذ الإجراء نفسه على نحو معاكس. من هنا — على سبيل المثال — يتم تمثيل كلمة GET بالأحرف **ZTP** في النص المشفَّر، فيما يتم تمثيل كلمة BIG في النص المشفَّر بالأحرف **IYZ**. لاحظ، على ذكر هذا المثال، أن شفرة قيصر تعتبر حالة خاصة

من شفرات الاستبدال البسيط؛ إذ لا يعدو الترتيب الذي جرت معه كتابةُ الأحرف بالخط العريض مجرد عملية إزاحة للحروف الأبجدية.

يساوي عدد مفاتيح شفرات الاستبدال البسيط عدد طرق ترتيب الأحرف الستة والعشرين الهجائية، وهو ما يطلق عليه مضروب العدد 26 (وهو حاصل ضرب جميع الأعداد الصحيحة الموجبة التي تقل عن 26 أو تساويه)، ويُشار إليه بالرمز !26 أيْ $1 \times 2 \times 3 \times \cdots \times 24 \times 25 \times 26$؛ أيْ ما يساوي:

403,291,461,126,605,635,584,000,000

هذا لا شك رقم كبير وليس من المحتمل أن يحاول أحد التوصل إلى المفتاح من خلال إجراء عملية بحث شاملة. لكن وجود مثل هذا العدد الضخم من المفاتيح له مشكلاته، وهناك فضلًا عن ذلك عددٌ من الملاحظات تتصل بمشكلات إدارة المفاتيح التي تصاحب استخدام شفرات الاستبدال البسيط. تتمثل الملاحظة البديهية الأولى في طول وصعوبة تذكُّر المفتاح، على خلاف شفرة قيصر؛ من ثَمَّ، عندما كان هذا النوع من الأنظمة يُستخدم يدويًّا، في عصر ما قبل الكمبيوتر، كانت تجري عادةً كتابةُ المفتاح في ورقة. وفي حال الاطلاع على هذه الورقة و/أو سرقتها، يجري اختراق النظام. وفي حال فقدان الورقة «تُفقد» جميع الرسائل المشفَّرة؛ بمعنى أنه كان يتعين على المتلقي المقصود للرسائل أن يتولى كسر الخوارزمية لبيان محتوى الرسائل.

للتغلب على هذا النوع من المخاطر، حاول المستخدمون اكتشاف أساليب لتصميم مفاتيح يسهُل تذكرها. كان أحد هذه الأساليب يتمثَّل في التفكير في «جملة المفتاح»، والتخلص من جميع الحروف المتكررة، وجعل هذه الصيغة هي «بداية» تصميم المفتاح، ثم التوسع في تصميم المفتاح من خلال إضافة الأحرف المتبقية مرتبة هجائيًّا. لذا — على سبيل المثال — إذا كانت جملة المفتاح We hope you enjoy this book (نأمل أن تستمتع بقراءة هذا الكتاب) تصبح بداية المفتاح بالتخلص من الحروف المتكررة wehopyunjtisbk؛ ومن ثَمَّ يصير المفتاح كاملًا:

W E H O P Y U N J T I S B K A C D F G L M Q R V X Z

بديهيًّا، حصْر المفاتيح على تلك التي يمكن اشتقاقها من جملة المفتاح يقلل عدد المفاتيح؛ إذ لا يمكن اشتقاق نسبة كبيرة من مفاتيح شفرات الاستبدال البسيط الخاص بمضروب 26! من جملة إنجليزية على هذا النحو. ومع ذلك لا يزال عدد المفاتيح كبيرًا للغاية؛ بحيث يتعذر إجراء بحث شامل عن المفتاح الصحيح ويكون من السهل تذكر المفتاح الآن.

تتمثل الملاحظة الثانية فيما يتعلق بنظام شفرات الاستبدال البسيط في وجود احتمال أن يؤدي تشفير الرسالة نفسها من خلال عدد كبير من المفاتيح إلى نص مشفَّر واحد. هَبْ — على سبيل المثال — أنَّ الرسالة هي: MEET ME TONIGHT (لنلتقِ الليلة)؛ إذا استخدمنا المثال الأول للمفتاح، يصبح النص المشفَّر **FTTP FT PREYZSP**. ومع ذلك يصدر عن أي مفتاح يحول E إلى **T**، وG إلى **Z**، وH إلى **S**، وI إلى **Y**، وM إلى **F**، وN إلى **E**، وO إلى **R**، وT إلى **P** النص المشفَّر نفسه. وهكذا يكون هناك العدد التالي من المفاتيح التي تعطي نفس النص المشفر:

$$18! = 6,402,373,705,728,000$$

يعني ذلك، على الأقل بالنسبة إلى هذا النوع من التشفير، أننا يجب ألا نفترض حاجة الطرف المعترض إلى تحديد المفتاح كاملًا قبل الحصول على رسالتنا الأصلية عبر نص مشفَّر جرى اعتراضه.

قبل أن نناقش كيف يستطيع طرفٌ معترضٌ استغلالَ إحصاءات اللغة الإنجليزية لاعتراض عدد من الشفرات، بما في ذلك شفرات الاستبدال البسيط، نبين أولًا بعض خصائص شفرات الاستبدال البسيط من خلال أربعة أمثلة صغيرة منتقاة بعناية. في الأمثلة التالية نفترض اعتراض أحد الأطراف — الذي يعرف أن الرسالة مكتوبة باللغة الإنجليزية مثلما هو على علم باستخدام نظام شفرات الاستبدال البسيط — للنصوص المشفَّرة.

(٣-١) مثال ١: G WR W RWL

بما أن الإنجليزية لا تحتوي على كلمات تتألف من حرف واحد سوى كلمتين اثنتين فقط، فمن المنطقي افتراض أن **G** تمثِّل A و**W** تمثِّل I أو العكس. ومن السهولة بمكان

استبعاد احتمال أن **G** تمثِّل A؛ ومن ثَمَّ نخلُص سريعًا من ذلك إلى أن الرسالة تبدأ هكذا I AM A MA، وأن هناك عددًا محدودًا من الاحتمالات بالنسبة للحرف الأخير. إذا افترضنا أننا نعرف أن الرسالة هي عبارة عن جملة تامة باللغة الإنجليزية فمن شبه المؤكد أن الرسالة هي I AM A MAN. من الأهمية بمكان إدراك أن هذا الاستدلال البسيط لا يستعين بأي أساليب لتحليل الشفرات؛ إذ «يخضع» هذا الاستدلال بصورة أو بأخرى لتراكيب اللغة الإنجليزية. لاحظ أيضًا أنه على الرغم من عدم تحديد المفتاح عن طريق هذا الاستدلال، فإنه يقلل عدد احتمالات المفاتيح من 26! إلى 22! إذا كانت الجملة السابقة هي بداية رسالة أطول، فسنحتاج إلى حجج أخرى لتحديد باقي المفتاح أو إلى إجراء عملية بحث محدودة عن المفتاح وإن كانت غير ممكنة حسابيًّا. نلاحظ أيضًا أنه كان من الشائع عمليًّا منع هذا النوع من الهجمات عن طريق نقل الأحرف في مجموعات تتألف من خمسة أحرف؛ ومن ثَمَّ إخفاء جميع المعلومات التي تتعلق بطول و/أو نهايات الكلمات.

(٣-٢) مثال ٢: HKC

ماذا يمكن أن نقول؟ ليس كثيرًا. بما أنه ليس هناك معلومات أخرى، قد تشير الرسالة إلى أي متتالية ذات معنًى من ثلاثة أحرف متمايزة. بالطبع يمكننا أن نستبعد بعض المفاتيح، لنقْل تلك المفاتيح التي تشفِّر Z إلى **H**، وQ إلى **K**، وK إلى **C** آنيًّا. في المقابل، لا يزال عدد الاحتمالات المتبقية كبيرًا للغاية؛ ما يجعلنا نُستدرج إلى القول بأن مجرد اعتراض النص المشفَّر هذا لا يفيدنا في شيء. من الصحيح تمامًا أننا إذا أردنا إرسال رسالة واحدة تتألف من ثلاثة أحرف فقط، فستبدو شفرات الاستبدال البسيط مناسبةً، وأن إجراء عملية بحث شاملة للنص المشفَّر سيسفر عن جميع الكلمات المؤلفة من ثلاثة أحرف (بأحرف متمايزة) كرسائل محتملة.

(٣-٣) مثال ٣: HATTPT

في هذا المثال، نستطيع بالتأكيد حصر عدد الاحتمالات لعدد حروف النص الأصلي التي قد تُحول إلى الحرف **T**. ربما نستطيع أيضًا الاستنباط في يقين أن أحد أحرف **T** أو **P** في

المثال تمثِّل حرفًا متحركًا. بالإضافة إلى ذلك، إذا كان لدينا ما يجعلنا نعتقد أن الرسالة المُعترضة هي عبارة عن كلمة واحدة كاملة، فربما سنتمكن من كتابة جميع الاحتمالات. بعض الأمثلة على ذلك كالآتي: CHEESE، وMISSES، وCANNON.

(٣-٤) مثال ٤: HATTPT (مع ملاحظة أن الرسالة عبارة عن اسم دولة)

في هذا المثال، نعتقد أن الرسالة يجب أن تكون GREECE. يتمثَّل الفرق بين المثالين ٣ و٤ في توافر بعض المعلومات الإضافية في المثال ٤، وهو ما جعل من مهمة الطرف المعترض سهلة بدلًا من «مستحيلة». بطبيعة الحال، يعتبر ذلك إحدى مهام إدارات الاستخبارات في «حالات الحرب»؛ إذ تُعتبر المعلومات الاستخباراتية التي توفرها هذه الإدارات العاملَ الحاسم في تمكين مُحلِّلي الشفرات من فك شفرة العدو.

(٤) إحصاءات اللغة الإنجليزية

كانت الأمثلة في القسم السابق جميعها قصيرة وجرى انتقاؤها بعناية لبيان نقاط محددة. لكنه، حتى في حال استخدام شفرات الاستبدال البسيط لتشفير مقاطع طويلة من نص إنجليزي، يوجد عدد من أساليب الاعتراض المباشر التي تسمح بالكشف عن محتوى الرسالة والمفتاح، أو على الأقل الجزء الأكبر من المفتاح. تستعين أساليب الاعتراض هذه بخصائص معروفة في اللغة الإنجليزية. يبين جدول ٣-٢ معدلات التكرار، في صورة نسب، لأحرف الهجاء في عينة تتألف من أكثر من 300 ألف حرف مأخوذة من مقاطع في عدد من الصحف والروايات. (يعتمد هذا الجدول على جدول آخر نُشر في كتاب «أنظمة التشفير: حماية الاتصالات» لمؤلِّفَيْه إتش جيه بيكر وإف سي بايبر.)

يتماشى تمثيل الأحرف في هذا الجدول مع العديد من الجداول الأخرى التي وضعها مؤلفون آخرون؛ إذ يمكن تفسير هذه الأحرف على أنها تمثِّل معدلات التكرار المتوقعة للأحرف في أي نص إنجليزي. تُظهر هذه الإحصائيةُ بجلاءٍ احتماليةَ هيمنةِ عدد محدود للغاية من الأحرف على أي نص إنجليزي.

جدول ٣-٢: معدلات التكرار النسبية المتوقعة للأحرف في نص إنجليزي.

حرف	٪	حرف	٪
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	2.0
L	4.0	Y	0.1
M	2.4	Z	0.1

عند استخدام شفرات الاستبدال البسيط، يحلُّ محلَّ كل حرف من حروف الأبجدية الحرفُ نفسه الذي جرى استبداله، أيًّا كان موضعه في النص. من ثم، إذا استخدمنا تشفيرًا — على سبيل المثال — يحل فيه حرفُ **R** محلَّ حرف E، فسيظل معدل تكرار حرف **R** في النص المشفَّر مساويًا لمعدل تكرار حرف E في الرسالة؛ وهو ما يعني أنه إذا عَكَسَ جدولُ ٣-٢ معدلَ تكرار الحروف في رسالةٍ ما، فستُظهر معدلاتُ تكرار الأحرف في النص المشفَّر عدمَ التوازن نفسه، وإن كانت معدلات تكرار الأحرف موزعة على نحو مختلف بينها. لبيان ذلك أكثر، نعرض الرسم البياني لمعدلات تكرار الأحرف في نص مشفَّر طويل جرى الحصول عليه عن طريق شفرات الاستبدال البسيط.

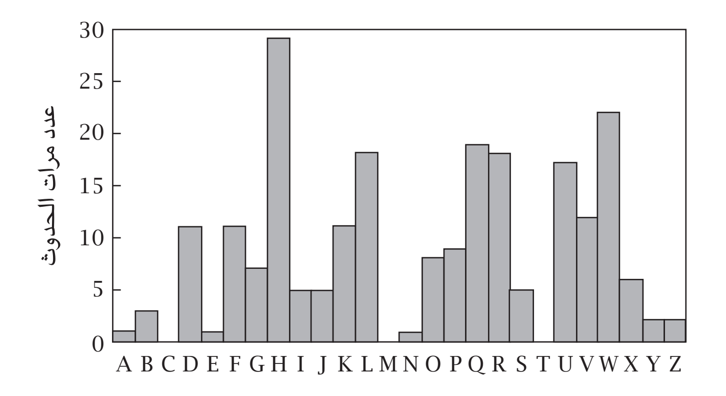
بمقارنة جدول ٣-٢ بهذا الشكل، ربما يستطيع أحد محللي الشفرات تخمين أن **H** تمثِّل E وأن **W** تمثل T. وبما أن أكثر الثلاثيات شيوعًا في اللغة الإنجليزية هي THE، فسيكتسب الطرف المعترض ثقة في هذا الافتراض من خلال التأكد مما إذا كان أكثر الثلاثيات شيوعًا في النص المشفَّر هو **W*H**؛ حيث تمثِّل * حرفًا ثابتًا — وهو ما لا يدعم محاولات التخمين الأولى فقط بل يشير إلى أن النص الأصلي المكافئ للحرف * هو H. من لديه اهتمام بمعرفة مدى سهولة فك هذه الشفرات، يجب أن يحاول قراءة الفقرة التالية التي جرى تشفيرها باستخدام شفرات الاستبدال البسيط:

> **DIX DR TZX KXCQDIQ RDK XIHPSZXKPIB TZPQ TXGT PQ TD QZDM TZX KXCJXK ZDM XCQPVN TZPQ TNSX DR HPSZXK HCI LX LKDUXI. TZX MDKJ QTKFHTFKX DR TZX SVCPITXGT ZCQ LXXI SKXQXKWXJ TD OCUX TZX XGXKHPQX XCQPXK. PR MX ZCJ MKPTTXI TZX. HKNSTDBKCOPI BKDFSQ DR RPWX VXTTXKQ TZXI PT MDFVJ ZCWX LXXI ZCKJXK. TD HDIWPIHX NDFKQXVWXQ DR TZPQ SCPKQ SCPKQ DR KXCJXKQ HCI SKDWPJX XCHZ DTZXK MPTZ HKNSTDBKCOQ MPTZ TZPQ VXTTXK BKDFSIB.**

كل قارئ استطاع فك شفرة بيان النص المشفر هذا لا شك استفاد من المعلومات التي وفرها وجود مسافات بين الأحرف. وكان فك الشفرة سيصبح أكثر صعوبة بكثير حال جرى حذف المسافات بين الأحرف الإنجليزية.

نختم هذه المناقشة القصيرة بالإقرار بأننا لم نحدد على وجه الدقة حجم النص المشفَّر الذي نعتبره «طويلًا». لا توجد بطبيعة الحال إجابة دقيقة. وفي حين يعتبر توفر 200 حرف كافيًا بكل تأكيد للاعتماد على نتائج الإحصاءات، وجدنا أن الطلاب يستطيعون فك شفرة رسالة يتضمن نص مشفَّرها 100 حرف أو أكثر.

كملاحظة جانبية، نؤكد على عدم وجود ضمانة في أن تتطابق الإحصاءات لأي رسالة مع الإحصاءات في جدول ٣-٢. على سبيل المثال، إذا جرى تشفير خطاب شخصي فمن الأرجح أن تظهر كلمة you (أنت) بكثرة مثل كلمة the (أداة التعريف «أل»). كمثال على



مدرج تكراري يوضح معدلات التكرار النسبية للأحرف في نص مشفَّر جرى الحصول عليه باستخدام شفرات الاستبدال البسيط.

كيفية التلاعب عمدًا بالإحصاءات في إحدى الرسائل، نجد رواية تتألف من 200 صفحة لا تحتوي على الحرف E (ترجمة جلبرت آدير لرواية «فراغ» لمؤلفها جورج بيرك).

يتمثَّل السبب في إمكانية وقوع اعتراض كالذي بيَّنَّاه توًّا في وجود أحرف شائعة «قليلة» من الأرجح أن «تهيمن» على الرسالة، وهو ما يجعل تحديد النص المكافئ لنص التشفير سهلًا. تتمثل إحدى طرق تجنب ذلك في إجراء عملية استبدال بسيطة على «الكلمات ثنائية الأحرف»؛ أي أزواج من الأحرف المتتالية. إذا فعلنا ذلك، فسيتألف المفتاح من ترتيب محدد من 676 كلمة ثنائية الأحرف، وهو ما سوف يعطينا مفاتيح طويلة للغاية وعددًا هائلًا من المفاتيح الممكنة قدرها 676! ومع ذلك ستكون مفاتيحُ مثلُ هذه مهلهلةً للغاية كما ستتعرض لنفس نوع الهجمات كما هو الحال في المفاتيح المؤلفة من أحرف فردية؛ إذ يهيمن على الرسائل الطويلة على الأرجح عددٌ محدود نسبيًّا من الكلمات ثنائية الأحرف.

بداهةً، لن يكون عمليًّا محاولةُ وضع قائمة بجميع الكلمات الثنائية البالغ عددها 676 كلمة أعلى النصوص المشفَّرة المكافئة لها؛ بعبارة أخرى، محاكاة تمثيل المفتاح الأصلي لشفرات الاستبدال البسيط. بناءً عليه، نحتاج إلى طريقة سهلة لتحديد المفاتيح

وللتعبير عن خوارزمية التشفير وفك التشفير. نضرب الآن مثلًا لشفرة تعتمد على الكلمات ثنائية الأحرف فيما نَستخدم عددًا محدودًا نسبيًّا من جميع المفاتيح الممكنة.

(٥) شفرة بلايفير

ابتكر «شفرة بلايفير» السير تشارلز وتستون والبارون ليون بلايفير في عام ١٨٥٤ وجرى استخدامها من قِبل إدارة الحرب البريطانية حتى بداية القرن العشرين، وقد استُخدِمَتْ في حرب البوير. وتُعد هذه الشفرة مثالًا على نظام شفرة «الكلمات ثنائية الأحرف»؛ وهو ما يعني تشفير الأحرف أزواجًا في مقابل تشفيرها مفردةً. يتمثَّل المفتاح في مربع يتألف من خمسة أحرف طولًا وعرضًا (يحتوي المربع على 25 حرفًا تتكون من خلال حذف حرف J من الأبجدية)؛ ومن ثَمَّ يكون لدينا المضروب 25! أو عدد مفاتيح يساوي:

$$15,511,210,043,330,985,984,000,000$$

قبل إجراء عملية التشفير باستخدام شفرة بلايفير يجب إعادة ترتيب الرسالة قليلًا. لتنفيذ ذلك، يجب:

- استبدال كل حرف I بحرف J.
- كتابة الرسالة في أزواج من الأحرف.
- عدم السماح بوجود أزواج أحرف متطابقة، وإن وجدت يُدرَج حرف Z بينها.
- إضافة حرف Z في النهاية، إذا كان عدد الأحرف فرديًّا.

لبيان طريقة عمل نظام شفرة بلايفير سنختار مفتاحًا محددًا لا يوجد ما يميز اختيارنا له:

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

بمجرد إعادة ترتيب الرسالة على نحو مناسب، نعرض قاعدة التشفير في نظام شفرة بلايفير. لبيان طريقة التشفير سنتوسع في تصميم المفتاح بإضافة عمود سادس وصفٍّ سادس للمفتاح الأصلي. ويتطابق الصف السادس مع الصف الأول، في حين يتطابق العمود السادس مع العمود الأول؛ من ثَمَّ — على سبيل المثال — يمكن التوسع في تصميم مفتاح كما هو موضح في الشكل:

S	T	A	N	D	S
E	R	C	H	B	E
K	F	G	I	L	K
M	O	P	Q	U	M
V	W	X	Y	Z	V
S	T	A	N	D	

تتلخص قاعدة التشفير في نظام شفرة بلايفير في الآتي:

- إذا وقع الحرفان في الصف نفسه من مربع المفتاح، يحل محل كل حرف الحرفُ الذي إلى يمينه في مربع المفتاح الممتد.
- إذا وقع الحرفان في العمود نفسه من مربع المفتاح، يحل محل كل حرف الحرفُ الذي يقع إلى الأسفل منه في مربع المفتاح الممتد.
- إذا لم يقع الحرفان في الصف أو العمود نفسه، يحل محل الحرفِ الأول الحرفُ الذي يقع في صف الحرف الأول وعمود الحرف الثاني. ويحل محل الحرف الثاني الحرفُ الذي في الركن الرابع من المستطيل الذي تشكَّل من الحروف الثلاثة المُستخدمة حتى الآن.

نشفِّر الآن الرسالة التالية: GOOD BROOMS SWEEP CLEAN (المكانس الجيدة تنظِّف جيدًا).

بما أنه ليس هناك أي حروف J في الرسالة فلا يجب سوى كتابة الرسالة في أزواج من الأحرف مع وضع أحرف Z زائدة متى كان ذلك لازمًا. نحصل بناءً على ذلك على الآتي:

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

وهكذا، بالنسبة إلى المفتاح الذي صممناه؛ GO تصبح **FP**، وOD تصبح **UT**، وOM تصبح **PO**. يصبح النص المشفَّر الكامل كالآتي:

FP UT EC UW PO DV TV BV CM CM BG CS DY

مثلما هو الحال مع شفرات الاستبدال البسيط، مال المستخدمون إلى الاستعانة بجملة سرية لتحديد مصفوفة المفتاح. كان الأسلوب المتبع في فك الشفرة في نظام شفرة بلايفير هو نفسه المتبع في شفرات الاستبدال البسيط، والذي يتمثل في كتابة الجملة السرية، ثم التخلص من الأحرف المتكررة، ثم إضافة الأحرف غير المستخدمة في ترتيب أبجدي. لذا، إذا كانت الجملة السرية UNIVERSITY OF LONDON (جامعة لندن) نحصل على UNIVERSTYOFLD عند التخلص من الأحرف المتكررة، ويمكن ترتيب الأحرف في مربع المفتاح مثلما هو موضح في الشكل التالي:

U	N	I	V	E
R	S	T	Y	O
F	L	D	A	B
C	G	H	K	M
P	Q	W	X	Z

تعتبر عملية فك التشفير، مثلما هو الحال دومًا، عملية عكسية لعملية التشفير. من يرغب من القرَّاء في التأكد من فهم طريقة عمل نظام شفرة بلايفير عليه أن يحاول فك شفرة **MBOUBTZE** باستخدام مربع المفتاح التالي. (الإجابة هي كلمة إنجليزية تتألف من سبعة أحرف نأمل ألا تعكس الحالة المزاجية للقارئ.) لا نهدف إلى الحديث عن تحليل هذه الشفرة. هناك أمثلة أخرى كثيرة لشفرات يسهُل وضعها ومحاولة فكها. وتوجد في نهاية هذا الكتاب مراجع مناسبة حول التشفير.

(٦) الترميز المتناغم

يتمثل خيار آخر لتطوير نظام شفرات الاستبدال البسيط في التوسع في الأحرف الهجائية من خلال إضافة بعض الرموز الزائدة؛ بحيث يُمثَّل — على سبيل المثال — حرف النص الأصلي E بأكثر من رمز في نص التشفير.

يُطلق على هذه الرموزِ الزائدةِ العناصرُ العشوائيةُ، كما تُسمى عملية التوسع في الأحرف الهجائية بعملية الترميز المتناغم. لبيان ذلك، نطرح شفرة تكون فيها عناصر النص المشفَّر هي الأعداد 00، 01، 02، ...، 31. يمثِّل كل عدد في النص المشفَّر حرفًا واحدًا فقط في النص الأصلي، لكن كل حرف من الأحرف A وE وN وO وR وT يجري تمثيله برمزين مختلفين.

لبيان ذلك أكثر، نخصص أعدادًا للأحرف مثلما هو موضَّح في الشكل التالي:

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
01	07	14	21	04	13	27	20	29	31	06	28	12	30	17	00

N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
18	26	19	09	10	25	23	02	08	24	22	05	16	15	11	03

إذا فعلنا ذلك، فقد يصبح من الممكن كتابة كلمة TEETH، التي تحتوي على زوجين من الأحرف المتكررة، كالآتي: 31 08 13 27 24. لمن لا يعرف المفتاح، تعتبر الأعداد الخمسة المكونة للنص المشفَّر مختلفة لكن لن يكون هناك احتمال لتعرُّض المتلقي الحقيقي للرسالة للارتباك.

الأرجح أن تكون الأحرف الستة المنتقاة هي الأحرف الستة الأكثر انتشارًا في النص الأصلي. على سبيل المثال، إذا كان قرار تحديد أيٍّ من العددين المُنْتَقَيَيْنِ يمثل الحرف E قرارًا عشوائيًّا، فسنتوقع أن «يشغل» كلٌّ من العددين حوالي ٦٪ من النص المشفَّر. وعلى وجه العموم، تتمثل نتيجة استخدام الترميز المتناغم في ضمان أن يكون المدرج التكراري المتوقع للنص المشفَّر أكثر انبساطًا من المدرج التكراري للنص الأصلي، وهو ما يجعل عملية الاعتراض من خلال استخدام الإحصاءات اللغوية أكثر صعوبة.

ملاحظة ١: في هذه الشفرة، نكتب 00، 01، 02 لنمثل الأعداد 0، 1، 2 ... إلخ. ففي أي وقت لا تُستخدم فيه المسافات، يُستخدم هذا النوع من التمثيل الرقمي للتمييز بين «اثني عشر» و«واحد يليه اثنان» على سبيل المثال.

ملاحظة ٢: يعتبر كسر شفرات الاستبدال البسيط سهلًا نسبيًّا ونأمل في أن جميع القرَّاء تمكنوا من فك شفرة فقرة النص المشفَّر عاليَهُ. أما هذا النوع من التشفير الذي نناقشه فيتطلب الكثير من الصبر والحظ. يجب أن يحاول كلٌّ مَن يحتاج إلى الاقتناع أو الاستمتاع بفك هذا النوع من الشفرات قراءة النص المشفَّر التالي. تتمثل المعلومات الوحيدة المتوفرة بشأن النص المشفَّر هذا في أن نصًّا إنجليزيًّا جرى تشفيره باستخدام شفرات الاستبدال البسيط بالاستعانة بنظام التشفير المتناغم كما سبق توضيحه أعلاه. المفتاح غير معروف، وهو ليس المفتاح المذكور سابقًا. بالإضافة إلى ذلك، كُتبت الأحرف في مجموعات من خمسة أحرف. (وهو ما يعني عدم قدرة الطرف المعترض على تحديد الكلمات القصيرة، خاصةً تلك التي تتألف من حرف واحد.) لا يعتبر فك مثل هذا النوع من الشفرات مسألة سهلة، ويجب ألا يشعر القراء بضرورة التزامهم بفكها.

24	29	25	00	20	01	12	27	10	01	12	06	29	07	08
31	29	05	07	14	20	26	01	04	26	20	06	28	29	28
05	04	31	28	18	30	01	31	21	26	25	24	26	12	29
04	26	31	18	23	15	21	25	26	31	28	26	30	10	01
21	07	31	18	16	12	12	28	18	13	05	08	21	24	30
20	21	25	24	21	30	10	18	17	19	31	28	18	05	12
31	05	24	09	21	08	26	05	08	14	12	17	27	07	04
18	20	08	12	05	25	04	13	27	31	12	28	18	19	05
24	31	12	28	05	12	12	28	18	08	31	01	12	21	08
31	21	24	08	05	23	18	19	10	01	12	12	26	23	15
26	05	25	08	21	31	21	08	07	29	12	08	29	26	05
08	14	12	17	21	04	26	25	12	21	19	14	31	28	18
30	17	30	27	10	01	20	10	26	31	12	26	20	08	21
25	12	28	18	30	10	05	21	07	12	18	16	31	30	01
12	21	18	25	24	26	01	07	04	10	27	24	09	05	23

26	13	29	31	28	11	18	20	14	21	15	30	29	20	12
01	07	31	19	17	23	12	28	26	24	23	14	30	12	01
07	01	10	14	08	12	21	25	19	01	24	31	13	20	18
05	09	21	07	00	24	21	30	28	26	20	08	27	08	27
05	10	10	14	21	07	11	29	10	11	18	08	01	15	21
16	31	27	23	26	17	19	08	24	21	18	25	12	21	19
21	24	20	18	01	08	17	07	21	25	00	05	25	04	21
07	08	30	21	20	18	04	00	27	26	08	08	06	17	23
09	21	07	12	28	21	08	24	17	25	31	18	16	31	06
26	25	17	12	18	31	28	01	12	31	28	26	24	20	14
30	12	17	00	20	01	30	28	21	24	12	18	05	15	18
15	30	10	29	14	18	04	01	31	13	10	26	12	24	28
10	26	14	30	05	23	09	21	07	24	10	27	04	26	04
30	26	17	30	10	26	06	21	12	28	05	07	01	30	31
21	31	27	04	18	19	17	23	24	20	17	08	08	06	17
20	04	30	27	03	03	10	26	08						

(٧) التشفير متعدد الأحرف

عند استخدام الترميز المتناغم، يصبح المدرج التكراري للنص المشفَّر أكثر انبساطًا من خلال زيادة عدد الأحرف الهجائية، وهو ما يضمن تمثيل أكثر من رمز في النص المشفر لنفس الحرف في النص الأصلي. ومع ذلك يظل صحيحًا أن كل رمز في نص التشفير يمثِّل حرفًا وحيدًا في النص الأصلي، وهو ما يمثِّل دائمًا خطرًا في أن يؤلف الطرف المعترض قاموسًا يحتوي على أزواج معروفة من النص المشفر والنص الأصلي لمفتاح معين.

هناك أسلوب آخر لتحقيق هدف جعْل المدرج التكراري للنص المشفَّر منبسطًا من خلال استخدام شفرة متعددة الأحرف. فعند استخدام التشفير متعدد الأحرف، قد يختلف الرمز في نص التشفير الذي يحل محل حرف محدد في النص الأصلي عبر النص المشفَّر، بل وقد يعتمد — على سبيل المثال — في تمثيله على موضعه في رسالة النص

الأصلي أو محتوى النص الأصلي الذي يسبقه. بالنسبة إلى هذا النوع من الشفرات، قد يمثِّل الرمز ذاته في النص المشفر عدة أحرف مختلفة في النص الأصلي، وهو ما لا ينطبق في حال الترميز المتناغم.

نعيد فنؤكد مرة أخرى أن الأمثلة البسيطة التي نضربها لهذه الشفرات لم تعد مستخدمة الآن. ومع ذلك نعرضها في شيء من التفصيل؛ إذ يمكننا من خلال ذلك الإشارةُ إلى بعض أوجه الضعف فيها التي يجب على مصمم الخوارزميات الحديثة أن يتجنبها. مثلما هو الحال في الأمثلة السابقة، نتناول هذه الأمثلة لعرض عدد من أساليب تحليل الشفرات، ونظرًا لأنها تمكننا من وضع تمارين تزيد من معرفتنا فضلًا عن استمتاعنا بها.

(٨) شفرة فيجنر

لعل أفضل الطرق اليدوية المعروفة للشفرات متعددة الأحرف هي «شفرة» فيجنر، التي جاء اسمها من بليز دي فيجنر، وهو دبلوماسي فرنسي عاش في القرن السادس عشر. وعلى الرغم من نشر هذه الشفرة في عام ١٥٨٦، لم يجْرِ الإقرار بها على نطاق واسع إلا بعد مرور مائتي عام؛ وكان كسرها بواسطة باباج وكاسيسكي في منتصف القرن التاسع عشر. من المثير الإشارة إلى أن شفرة فيجنر جرى استخدامها من قِبَل جيش الكونفدرالية في الحرب الأهلية الأمريكية. وقد وقعت الحرب الأهلية بعد كسر شفرة فيجنر، وهو ما تشير إليه مقولة الجنرال يوليسيس إس جرانت: «ربما يستغرق فك شفرة المراسلات التي يجرى اعتراضها وقتًا أكثر من اللازم بحيث لا نحصل على أي فائدة منها، لكننا نحصل منها في بعض الأحيان على معلومات مفيدة.»

تَستخدم شفرة فيجنر مربع فيجنر لإجراء عملية التشفير. يحتوي العمود الأيسر (المفتاح) لهذا المربع على الأحرف الهجائية الإنجليزية، ولكل حرف منها، يتضمن الصف الذي يحدده الحرف تكرارًا للأبجدية بدءًا من هذا الحرف. لذا، يعطي كل حرف في العمود الأيسر شفرة قيصر بحيث يتحدد عدد حركات الإزاحة وفق ترتيب هذا الحرف في الأبجدية. على سبيل المثال، يعطي حرف g شفرة قيصر ذات 6 حركات إزاحة.

يتمثل أحد أكثر الأساليب شيوعًا في استخدام المربع للحصول على شفرة في انتقاء كلمة المفتاح (أو جملة المفتاح) لا تشتمل على أحرف متكررة. وإذا كانت رسالة النص

Key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

(Plaintext)

مربع فيجنر.

الأصلي أطول من المفتاح، نحصل، إذن، من خلال تكرار المفتاح كلما كان ذلك ضروريًّا، على متسلسلة من الأحرف تساوي في طولها طول الرسالة. على سبيل المثال، إذا كانت الرسالة PLAINTEXT وكانت كلمة المفتاح **fred** نحصل على الآتي:

الرسالة: P L A I N T E X T

المفتاح: **f r e d f r e d f**

نستخدم المربع الآن في تشفير الرسالة كما يلي:

لتشفير الحرف الابتدائي P نستخدم الحرف المفتاحي الذي يقع أسفله؛ وهو **f** في هذه الحالة. من ثم، لتشفير الحرف P ننتقل إلى صف المربع الذي يحدده الحرف **f** ونقرأ الحرف الواقع إلى أسفل حرف P؛ وهو حرف **U**. بالمثل، نشفِّر الحرف L عن طريق أخذ

الحرف الذي يقع أسفله في الصف الذي يحدده الحرف **r**؛ أي حرف **C**. نبيِّن عملية تشفير الحرف P عن طريق الحرف المفتاحي **f** في الشكل التالي:

Key	Plaintext																									
	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

استخدام مربع فيجنر لتشفير الحرف P عن طريق الحرف المفتاحي **f**.

كل قارئ يفرغ من عملية التشفير هذه سيخلُص إلى أن النص المشفَّر الكامل للنص الأصلي PLAINTEXT باستخدام كلمة المفتاح **fred** هو **UCELSLIAY**.

وهو ما يعني أننا صار لدينا ما يلي:

الرسالة:	P L A I N T E X T
المفتاح:	**f r e d f r e d f**
نص التشفير:	**U C E L S L I A Y**

نستطيع الآن أن نرى أن حرف النص الأصلي T يمثله حرفا **L** و**Y** في النص المشفر، وأن حرف النص المشفر **L** يمثل الحرفين I وT. من هنا، يبدو جليًّا أنه باستخدام هذه الشفرة، نستطيع الحيلولة دون تماثل أنماط معدلات تكرار الأحرف في النص المشفَّر مع نظيراتها في النصوص المشفَّرة في شفرات الاستبدال البسيط.

هناك تنويعات كثيرة لشفرة فيجنر، بما في ذلك شفرة يُسمح فيها بتكرار الأحرف في الكلمة المفتاحية. ويكون لكل نوع خصائص يختلف كلٌّ منها عن الآخر قليلًا؛ وهو ما يؤدي إلى اختلاف نوع الهجمات التي يتعرض لها. ومع ذلك نركِّز اهتمامنا على نظام الشفرة الذي حددناه هنا.

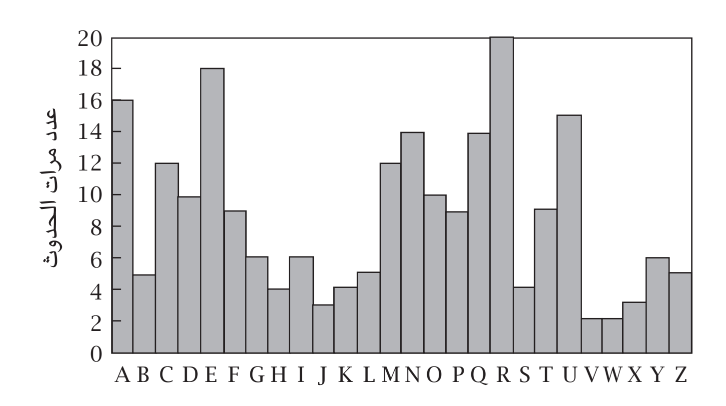
تعتبر شفرة فيجنر مثالًا خاصًّا على الشفرة متعددة الأحرف يجري فيه استخدام متسلسلة (قصيرة) من شفرات الاستبدال البسيط بنظام تكراري دقيق. ويُطلق على عدد مكونات الشفرة المستخدمة في شفرة فيجنر «دورة»، ومن الواضح أن الدورة في نسخة شفرة فيجنر التي عرضناها تعادل طول كلمة المفتاح.

قبل مواصلة حديثنا عن الشفرات الدورية، من الجدير بالذكر الأخذُ في الاعتبار أن الشفرة متعددةَ الأحرف التي تبلغ دورتها 3 لا تعدو أكثر من حالة خاصة من شفرة استبدال بسيط لنص ثلاثي الأحرف. لا تعدو هذه الملاحظة البسيطة أكثر من حالة خاصة للمبدأ العام القائل بأن تغيير أحرف الأبجدية قد يؤدي إلى تغيير «طبيعة» الشفرة. في الوقت الحالي، نركِّز على الشفرات التي تستخدم الأحرف الهجائية الإنجليزية رموزًا لها. وعند تناول أنظمة الشفرات الأكثر حداثة، غالبًا ما ننظر إلى جميع الرسائل باعتبارها متسلسلة من أرقام ثنائية (تتألف من أصفار وآحاد).

مثلما ذكرنا، يرجع أحد أسباب استخدام التشفير متعدد الأحرف إلى الرغبة في إخفاء معدلات تكرار الأحرف للُّغة المستخدمة. كمثال على ذلك، نعرض رسمًا بيانيًّا لتوضيح عدد معدلات تكرار الأحرف في نص مشفَّر جاء نتاج استخدام شفرة فيجنر دورتها 3 لتشفير نص إنجليزي.

هناك عدد من الاختلافات الواضحة بين هذا المدرج التكراري وذلك الموضَّح سابقًا. تتمثل أبرز هذه الاختلافات في أن كل حرف من الحروف الهجائية يظهر في المدرج التكراري الثاني، وعدم هيمنة أي حرف في هذا المدرج التكراري مثلما هيمن الحرف **H** على المدرج التكراري السابق. ويعد هذا المدرج التكراري أكثر انبساطًا من الشكل السابق؛ ومن ثَمَّ، لا يساعد الطرف المعترض المحتمل كثيرًا. قد يميل كلٌّ مَن ينظر إلى

المدرج التكراري الثاني إلى استنباط أن حرف **R** في النص المشفَّر يمثِّل حرف E في النص الأصلي في مكان ما، لكنه لن يَعرف في أي موضع حدث ذلك على وجه التحديد.



مدرج تكراري لنص مشفَّر عند استخدام ثلاث شفرات استبدال بسيط بتكرار دقيق.

بوجه عام، نتوقع أن يعكس انبساط المدرج التكراري طول الدورة، وأن زيادة طول الدورة تجعل فك الشفرة مسألة أصعب. يعتبر ذلك صحيحًا إلى حدٍّ ما. ومع ذلك يتمثَّل جُلُّ ما يحققه استخدام الشفرات متعددةِ الأحرف الدورية عمليًّا في ضمان زيادة حجم النص المشفَّر الذي يحتاجه محلل الشفرات للبدء في عملية اعتراض فعَّالة. لبيان ذلك، نركِّز على شفرة فيجنر. تعتبر بعض افتراضاتنا صحيحة فيما يتعلق بأيٍّ مِن الشفرات متعددة الأحرف، لكن بعض الافتراضات الأخرى تعتمد على الخصائص المتوفرة في تعريف شفرة فيجنر. من الأهمية بمكان أن يميز القارئ بين الحالتين. من هنا، قد يؤدي تغيير الشفرة متعددة الأحرف إلى تغيير تفاصيل عملية الاعتراض و«تقوية» النظام قليلًا. ومع ذلك تعتبر جميع الشفرات متعددة الأحرف، التي يكون المفتاح فيها أقصر من الرسالة، معرضة لبعض أنماط الاعتراض التي نعرضها هنا.

يكفي لكسر شفرة فيجنر تحديد كلمة المفتاح. في حال معرفة الدورة وفي حال عدم طولها على نحو مفرط، يمكن تحديد كلمة المفتاح من خلال كتابة برنامج حاسوبي لإجراء عملية بحث شاملة عن المفتاح. كمثال على ذلك، ربما يرغب القرَّاء في إجراء عملية

بحث عن المفتاح في النص المشفَّر **TGCSZ GEUAA EEWGQ AHQMC**، وذلك أخذًا في الاعتبار أن النص المشفَّر هذا هو نتاج استخدام شفرة فيجنر مع استخدام كلمة مفتاح دورتها 3 لتشفير فقرة من نص إنجليزي. سيواجه أي قارئ يحاول تنفيذ ذلك مسألة مثيرة للاهتمام تتمثل في تحديد كلمة المفتاح الصحيحة. يتمثل الافتراض الأساسي هنا في أن كلمة المفتاح هي كلمة تتألف من ثلاثة أحرف فقط تؤدي إلى التوصل إلى نص أصلي له معنًى. لكن المشكلة الحقيقية تتمثل في كيفية إدراك أن النص الأصلي يمثِّل نصًّا ذا معنًى. لعل أحد الاحتمالات يتمثَّل في الجلوس أمام الشاشة وفحْص نتيجة استخدام كل كلمة مفتاح. بطبيعة الحال، تعتبر هذه الطريقة مملَّة كما تستغرق وقتًا طويلًا. يجب العثور على بدائل أخرى.

عند إجراء عملية بحث شاملة عن كلمة مفتاح يبلغ طولها P، ربما يكون من السهولة بمكان تجربة جميع متسلسلات الأحرف P بصورة منهجية بدلًا من حصر عملية البحث في الكلمات الإنجليزية فقط. من هنا، بالنسبة إلى شفرة فيجنر التي تكون فيها قيمة الدورة P معلومة، ربما يتطلب إجراء عملية بحث شاملة إجراء 26^P محاولة؛ وهو ما يعني أن زيادة الدورة ستؤدي إلى خروج عملية البحث الشاملة عن نطاق السيطرة. لكنه في حال معرفة الدورة، سيصبح تحديد كلمة مفتاح مسألة مباشرة نسبيًّا دون حتى إجراء عملية بحث شاملة. تتمثَّل إحدى طرق تنفيذ ذلك في كتابة نص التشفير في صفوف تتألف من الحرف P؛ بحيث يجري إعادة بناء النص المشفَّر من خلال كتابة كل عمود بالترتيب. لذا — على سبيل المثال — عندما تكون $P = 3$ والنص المشفر هو $C_1C_2C_3C_4C_5C_6C_7C_8C_9\ldots$، سيُكتب كل عمود على النحو التالي:

$$C_1C_4C_7C_{10}\ldots$$

$$C_2C_5C_8C_{11}\ldots$$

$$C_3C_6C_9C_{12}\ldots$$

بمجرد الانتهاء من ذلك، سيصبح كل صف هو نتاج استخدام شفرة الاستبدال البسيط الذي يعتبر، بالنسبة لحالة شفرة فيجنر الخاصة، شفرةً مضافة. يمكن الآن استخدام الإحصاءات اللغوية في القسم السابق في كل صف من صفوف النص المشفَّر. حقيقةً، بالنسبة إلى شفرة فيجنر التي يعتبر النص المشفَّر فيها طويلًا مقارنةً بالدورة P،

ربما يكون كافيًا تحديد أكثر الأحرف تكرارًا في كل صف وافتراض تمثيله للأحرف E أو T، أو A. تعتمد الملاحظة الأخيرة على أن شفرة الاستبدال البسيط المستخدمة في كل صف إنما هي شفرة قيصر؛ وهو ما يعني، مثلما أشرنا، أن معرفة زوج واحد فقط من النص الأصلي والنص المشفر يعتبر كافيًا لتحديد كلمة المفتاح. بناءً عليه، إذا أمكن تحديد النص المشفر المكافئ لحرف واحد في كل صف، ربما من خلال مزيج من التخمين الذكي والحظ، فسيكون من الممكن تحديد كلمة المفتاح.

توحي المناقشة حتى الآن بأن المشكلة الحقيقية التي تواجه الطرف المعترض لشفرة فيجنر تتمثل في تحديد الدورة P. أحد الحلول هو تجربة جميع القيم الصغيرة للدورة P بصورة منهجية. لكنَّ هناك أيضًا عددًا من الطرق البسيطة المبتكرة التي يمكن من خلالها تحقيق ذلك. لعل أشهَر هذه الطرق على الإطلاق طريقة تُعرف باسم اختبار كاسيسكي، وهو الاختبار الذي استخدمه باباج، الذي كان أول من كسر الشفرة. كان أسلوبه يتمثَّل في البحث عن متسلسلة (طويلة) من الأحرف متكررة في النص المشفر. وعندما تظهر هذه المتسلسلات، تمثِّل على الأرجح مقاطع مطابقة للرسالة المشفَّرة باستخدام أحرف لوحة مفاتيح مطابقة، وهو ما يشير إلى أن الفجوات بين هذه الأنماط المتكررة ربما تمثِّل مضاعفات الدورة (تم تناول تحليل شفرة فيجنر تفصيلًا في كتاب «كتاب الشفرة» لسينج).

(٩) التشفير التبادلي

في جميع الأمثلة التي ذكرناها حتى الآن، جرى الاستعاضة عن أحرف، أو مجموعات من الأحرف في رسالة، بأحرف أو مجموعات من أحرف أخرى. من هنا، تقع جميع هذه الأمثلة تحت عنوان عام لشفرات الاستبدال. لكن توجد عائلات أخرى من أنظمة التشفير التي تقوم على فكرة تبديل ترتيب كتابة الأحرف، وهو ما يُعرف باسم «التشفير التبادلي». نضرب مثلًا بسيطًا على ذلك هنا.

في المثال الذي نضربه المفتاحُ هو رقم صغير. نستخدم رقم 5 كمفتاح. لتشفير رسالةٍ ما باستخدام هذا المفتاح، نكتب الرسالة في صفوف يتألف كلٌّ منها من خمسة

أحرف، ثم نجري عملية التشفير من خلال كتابة أحرف العمود الأول أولًا، ثم العمود الثاني، وهكذا. إذا لم يساوِ طولُ الرسالة أحدَ أضعاف رقم 5، نُضيف عددًا مناسبًا من حرف Z في النهاية قبل إجراء عملية التشفير. يمكن فهم عملية التشفير بسهولة بالغة من خلال مثال صغير.

نشفِّر الرسالة WHAT WAS THE WEATHER LIKE ON FRIDAY (كيف كانت حالة الجو يوم الجمعة). بما أن المفتاح هو 5، تتضمن الخطوة الأولى إذن كتابة الرسالة في صفوف يتألف كل صف منها من خمسة أحرف، كالآتي:

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	

بما أن طول الرسالة لا يساوي أحد أضعاف رقم 5، يجب إضافة حرف Z واحد لنحصل على النتيجة التالية:

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	Z

نقرأ الآن كل عمود على التوالي لنحصل على النص المشفَّر التالي:

WAWEEIHSERODATALNATHTIFYWEHKRZ

للحصول على مفتاح فك التشفير، نَقسِم طول الرسالة على المفتاح. في هذه الحالة، نقسم 30 على 5 لنحصل على 6. تصبح خوارزمية فك التشفير الآن مماثلة لخوارزمية التشفير. لذا — على سبيل المثال — نكتب النص المشفَّر في صفوف تتألف من 6 أحرف لنحصل على النتيجة التالية:

W	A	W	E	E	I
H	S	E	R	O	D
A	T	A	L	N	A
T	H	T	I	F	Y
W	E	H	K	R	Z

يسهُل الآن التحقق من أن قراءة كل عمود على التوالي سيفصح عن نص الرسالة الأصلية.

يسهُل كسر نوع الشفرات التبادلية المذكورة هنا. وبما أن المفتاح هو رقم يقسم طول النص المشفَّر، سوف يضطر الطرف المعترض إلى حساب طول النص المشفَّر وتجريب كل رقم يقبل القسمة عليه على التوالي.

(١٠) التشفير المعقَّد

إلى الآن في هذا الفصل، قدمنا عددًا من نماذج التشفير البسيطة يسهُل كسر شفرة معظمها. نعرض الآن لمفهوم يمكن استخدامه للمزج بين نوع أو اثنين من أنظمة التشفير الضعيفة نسبيًّا للحصول على نظام تشفير أقوى كثيرًا من أيهما، وهو ما يُعرف باسم «التشفير المعقَّد». يعتمد التشفير المعقَّد على فكرة بسيطة للغاية. هبْ أننا نريد أن نجري عملية تشفير معقدة باستخدام نظام الاستبدال البسيط ونظام التشفير التبادلي؛ سنشفِّر أولًا الرسالة باستخدام شفرة الاستبدال البسيط، ثم نشفِّر النص المشفَّر الناتج باستخدام التشفير التبادلي. سنطرح من خلال مثال بسيطٍ طريقةَ إجراء هذه العملية.

نشفِّر الرسالة ROYAL HOLLOWAY من خلال تشفيرها تشفيرًا معقدًا عن طريق تشفيرها أولًا باستخدام شفرة قيصر بمفتاح قيمته 2، ثم استخدام التشفير التبادلي

باستخدام مفتاح قيمته 4. بالنسبة إلى شفرة قيصر باستخدام مفتاح قيمته 2، نحصل على الآتي:

الرسالة: R O Y A L H O L L O W A Y
النص المشفَّر: **T Q A C N J Q N N Q Y C A**

بالنسبة إلى نظام التشفير التبادلي باستخدام مفتاح قيمته 4 نحصل على الآتي:

الرسالة: T Q A C N J Q N N Q Y C A
النص المشفَّر: **T N N A Q J Q Z A Q Y Z C N C Z**

يعتبر التشفير المعقد أسلوبًا في غاية الأهمية؛ إذ يمكن النظر إلى كثير من خوارزميات التشفير القوية الحديثة كنتاج لنظام التشفير المعقد باستخدام عدد من الخوارزميات الضعيفة نسبيًّا.

(١١) بعض النتائج

يبدو جليًّا من الأمثلة العديدة التي جرى تناولها في الأجزاء الأخيرة وجود العديد من العوامل التي تؤثر على فرص الطرف المعترض للرسائل في كسر شفرة نظام التشفير. رأينا أيضًا أنه على الرغم من أن أهم معلومة يريدها الطرف المعترض هي مفتاح فك التشفير، قد لا يحتاج الطرف المعترض إلى اكتشاف المفتاح بالكامل في حال إذا كانت لغة الشفرة تتسم ببناء محكم. في واقع الأمر، تشير الأمثلة الأولى التي عرضناها إلى أهمية عامل البناء اللغوي عند تقييم مدى نجاح الطرف المعترض في فك الشفرة. على سبيل المثال، إن إخفاء بيانات عشوائية أسهل بكثير مقارنة بتشفير نص إنجليزي بنجاح. بالنسبة إلى رسالة واحدة قصيرة، لنقل من ثلاثة أو أربعة أحرف، يوجد عدد كبير من خوارزميات التشفير الضعيفة التي تكفي على الأرجح لإخفاء محتوى الرسالة.

(١٢) ملحق

(١٢-١) مقدمة

في هذا الملحق، نناقش فكرتين رياضيتين أساسيتين؛ ألا وهما: التمثيلات الثنائية للأعداد الصحيحة، والمقياس الحسابي. تلعب كلتا الفكرتين دورًا محوريًّا في التشفير. غالبًا ما تدرَّس الأعداد الثنائية في المدارس والكليات، ولا يدرَّس المقياس الحسابي على نطاق واسع كالأعداد الثنائية، لكن في حال قيم خاصة مثل 7 و12، تعتبر عملية المقياس الحسابي عملية طبيعية يجريها الجميع.

(١٢-٢) الأعداد الثنائية

عندما يُكتب عدد صحيح بالنظام العشري نستخدم في الأساس خانة آحاد، وخانة عشرات، وخانة مئات، وخانة آلاف، وهكذا. من ثم، يشير رقم 3049 إلى 3 آلاف، و0 مئات، و4 عشرات، و9 آحاد. بالنسبة إلى الأعداد العشرية، نستخدم الأساس 10 فيما تمثل الخانات مضاعفات رقم 10؛ لذا $\mathbf{1} = 10^0$، $\mathbf{10} = 10^1$، $\mathbf{100} = 10^2$، $\mathbf{1000} = 10^3$، وهكذا.

بالنسبة إلى الأعداد الثنائية نستخدم الأساس 2. الرقمان الأساسيان هما 0 و1؛ حيث توجد خانة للآحاد، وخانة للأعداد الثنائية، وخانة للأعداد الرباعية (تذكر أن $2^2 = 4$)، وخانة للأعداد الثُّمانية $2^3 = 8$، وهكذا؛ وهو ما يعني إمكانية اعتبار كل مجموعة من الأعداد الثنائية رقمًا قائمًا بذاته. على سبيل المثال، 101 في النظام الثنائي يساوي 1 أربعة، و0 اثنان، و1 واحد؛ لذا فإن السلسلة الثنائية 101 تمثل $5 = 1 + 0 + 4$ في صورة عشرية. بالمثل، يمثِّل 1011 في صورة ثنائية = 1 ثمانية، و0 أربعة، و1 اثنان، و1 واحد. وهكذا، تمثِّل الكتلة الثنائية $11 = 1 + 2 + 0 + 8 = 1011$ في صورة عشرية. كمثال أخير، افترض الرقم 1100011. لدينا في هذه الحالة سبع خانات. مضاعفات العدد 2 هي 1، 2، 4، 8، 16، 32، 64؛ ومن ثَمَّ تمثِّل السلسلة الثنائية $99 = 1 + 2 + 0 + 0 + 0 + 32 + 64 = 1100011$ في صورة عشرية.

بداهةً، يمكن كتابة أي عدد صحيح موجب في صورة ثنائية، ويوجد العديد من الطرق التي تحدد هذه الصورة. نبين أحد هذه الأساليب من خلال مثالين. هَبْ أننا

نرغب في إيجاد التمثيل الثنائي للعدد 53؛ مضاعفات العدد 2 هي 1، 2، 4، 8، 16، 32، 64 ... لكن من الممكن أن نتوقف عند العدد 32؛ إذ إن جميع المضاعفات الأخرى أكبر من 53. يمكن الآن تمثيل 53 كالآتي: 21 + 32 = 53، كما يمكن تمثيل 21 هكذا: 5 + 16 = 21 وتمثيل 5 هكذا: 1 + 4 = 5. وبهذا يمكن تمثيل 53 على النحو التالي: 1 + 4 + 16 + 32 = 53. لا يعدو ما فعلناه سوى كتابة القيمة 53 في صورة مجموع مضاعفات الرقم 2. يمكن إذن تمثيل 53 كالآتي: = 53 $(1\times1) + (2\times0) + (4\times1) + (8\times0) + (16\times1) + (32\times1)$؛ ومن ثَمَّ تُمثَّل 53 هكذا: 110101 = 53 في صورة ثنائية. كمثال ثانٍ خذ العدد 86. في هذه الحالة، تكون أعلى قيمة لمضاعفات العدد 2 هي 64. بتكرار العملية السابقة، نجد أن 2+4+16+64 = 86؛ ومن ثَمَّ 86 هي 1010110 في صورة ثنائية.

يعتبر المصطلح bit اختصارًا يعبر عن الرقم الثنائي. فعندما نشير إلى عدد على أنه N-bits، نعني بذلك أن صورته الثنائية تتطلب عدد N من البِتات. على سبيل المثال، في الأمثلة السابقة، العدد 53 هو 6-bit و86 هو 7-bit. بوجه عام، يعطي العدد 3.32d فكرة عن عدد البتات المطلوبة للتعبير عن عدد عشري مكون من d من الأرقام في صورة ثنائية.

(١٢-٣) المقياس الحسابي

يهتم المقياس الحسابي بالأعداد الصحيحة فقط، وهي المعروفة باسم الأعداد الكاملة. فإذا كان العدد N عددًا صحيحًا موجبًا، إذن فلن يستخدم المقياس الحسابي N إلا الأعداد الصحيحة 0، 1، 2، 3، ...، N − 1؛ أي الأعداد الصحيحة من 0 إلى N − 1.

هناك عدد من قيم N التي يعتبر الرقم الحسابي القياسي N بالنسبة لها معروفًا لمعظم الناس، على الرغم من عدم معرفتهم بالمصطلحات الرياضية. على سبيل المثال، عندما نستخدم ساعة يقسِّم الوقت فيها إلى 12 ساعة زمنية، نستخدم الجمع للمقياس 12. إذا كانت الساعة الآن الثانية «فسيعرف» الجميع أن الساعة ستكون الخامسة في غضون ثلاث ساعات، مثلما ستكون الخامسة في غضون 15 ساعة؛ وذلك نظرًا لأن3 + 12 = 15؛ حيث يتكرر الوقت نفسه كل 12 ساعة. من الأعداد الطبيعية الأخرى N = 7 (لعدد أيام الأسبوع) وN = 2 (للأعداد الفردية والزوجية).

إذا تساوى عددان في المتبقي من حاصل قسمتهما على العدد N، نعتبرهما عددين متساويين بالنسبة للمقياس N. على سبيل المثال، إذا كانت $N = 7$، إذن، بما أن $2 + (7 \times 1) = 9$ و$2 + (7 \times 3) = 23$، نعتبر العددين 9 و23 متساويين بالنسبة للمقياس 7. وإذا كان X وY عددين متساويين قيمتهما N، نعبِّر عنهما هكذا: $X = Y$ (مقياس N). لاحظ إذن أن كل عدد صحيح يجب أن يساوي بالنسبة إلى المقياس N إحدى القيم: 0، 1، 2، ...، $N - 1$.

كمثال على استخدام المقياس الحسابي؛ هب أن اليوم الأول من الشهر هو يوم الثلاثاء؛ بديهيًّا إذنْ سيكون اليوم التالي هو يوم الأربعاء، والثالث هو الخميس، وهكذا. ماذا عن اليوم التاسع والعشرين؟ تتمثل إحدى طرق الإجابة على هذا السؤال في الرجوع إلى التقويم أو كتابة جميع أيام الشهر. تتمثَّل طريقة أخرى في ملاحظ نمط تكرار الأيام كل 7 أيام. بداهةً، سيكون اليوم الثامن هو يوم الثلاثاء أيضًا. نلاحظ الآن أن $1 + 7 \times 4 = 29$ التي تصبح $29 = 1$ (مقياس 7). وهكذا، يقع اليوم التاسع والعشرون بعد 4 أسابيع من اليوم الأول ويقع في يوم ثلاثاء. تظهر عملية مشابهة أنه حيث إن $5 + 7 \times 2 = 19$، يكون اليوم التاسع عشر هو يوم سبت.

متى عرضنا مفهوم المقياس N، يصبح إجراء العمليات الحسابية مسألة مباشرة. على سبيل المثال، إذا كانت $N = 11$، إذن $2 = 7 \times 5$ (مقياس 11) بما أن $5 \times 7 = 2 + (11 \times 3) = 35$. يمكن أيضًا كتابة معادلات الرقم الحسابي القياسي N. على سبيل المثال، يعني حل المعادلة $3X = 5$ (مقياس 8) إيجاد قيمة X بحيث يكون حاصل ضرب 3 في X يساوي 5 مقياس 8. حل هذه المعادلة هو: $X = 7$. تجدُر الإشارة إلى أن عرض أساليب لحل هذا النوع من المعادلات يقع خارج نطاق هذا الملحق. لكنه من السهولة بمكان التحقق من أن $X = 7$ تحقق المعادلة $3X = 5$ (مقياس 8)؛ حيث إن $5 + 8 \times 2 = 21 = 7 \times 3$. عند الحديث عن المقياس الحسابي، يجب تذكر عدم «جواز» استخدام أعداد سوى الأعداد الصحيحة؛ أي الأعداد الكاملة. وعلى وجه الخصوص، إذا طُلب منا حل معادلة مثل $3X = 5$ (مقياس 8)، يجب أن تكون الإجابة رقمًا صحيحًا يقع بين العددين 0 و7.

يرجع أحد الأسباب الرئيسية في الحديث عن المقياس الحسابي إلى أن اثنتين من أكثر خوارزميات المفتاح المعلن شيوعًا تستخدم الأس المقياسي باعتباره عمليتهما الرياضية الأساسية. يعني الأس المقياسي حساب X^a (مقياس N) للأعداد الصحيحة X، A، N. هب

أن $X = 5$، $A = 4$، $N = 7$؛ إذن، $5^4 = 5 \times 5 \times 5 \times 5 = 625 = (89 \times 7) + 2$؛ ومن ثَمَّ $5^4 = 2$ (مقياس 7). وفي حينِ لن يُضطر من يُجري عملية تشفير إلى إجراء أيٍّ من هذه العمليات الحسابية، تساعد هذه العمليات الحسابية في فهم طرق التمثيل الرمزي.

عند الحديث عن شفرة قيصر ذكرنا الشفرات الجمعية، التي تعتمد على تخصيص أعداد للأحرف الهجائية ثم استخدام المقياس 26. يشير التدقيق في مربع فيجنر إلى أن الصف الأول، الذي يحدده حرف المفتاح a، يمثِّل الشفرة الجمعية عن طريق صفر حركة إزاحة، بينما يمثِّل الصف الثاني، الذي يحدده حرف المفتاح b، شفرة جمعية عن طريق 1 حركة إزاحة وهكذا. في حقيقة الأمر، إذا ربطنا بين الأحرف والأعداد على نحو $A = 0, B = 1, \ldots, Z = 25$ فسيشير كل حرف مفتاح إلى استخدام شفرة جمعية تتحقق من خلال إجراء حركات إزاحة تساوي القيمة المرتبطة به. تعتبر هذه الملاحظة البسيطة مفيدة لكلِّ مَن يريد كتابة برنامج لتنفيذ شفرة فيجنر.

أعقب مناقشة الشفرات الجمعية تقديم لنظام شفرة ضربية؛ حيث أدرجنا تلك الأعداد التي يمكن استخدامها كمفاتيح. على الرغم من عدم وضوح كيفية حصولنا على القائمة، يسهُل التحقق من صحة القائمة مباشرةً. بالنسبة إلى الأعداد 1، 3، 5، 7، 9، 11، 15، 17، 19، 21، 23، 25، عندما نضرب الحروف الهجائية الستة والعشرين بهذه الأعداد المفتاحية، نحصل على 26 إجابة مختلفة؛ وهو ما يعني إمكانية استخدام هذه الأعداد كمفاتيح تشفير في نظام شفرة ضربية. نُدرج مفاتيح فك التشفير المقابلة في الأسفل، وعلى الرغم من عدم وضوح طريقة حسابها، يَسهُل التحقق من صحتها. تتمثل نتيجة الضرب في مفتاح التشفير ثم ضرب حاصل الضرب في مفتاح فك التشفير المقابل في عدم تغيير الأحرف، وهو ما يكافئ الضرب في رقم 1. على سبيل المثال، بالنسبة إلى مفتاح تشفير 3، ومفتاح فك تشفير 9، لا نحتاج إلا إلى إثبات أن $3 \times 9 = 1$ (مقياس 26)، وهو صحيح، بما أن $3 \times 9 = 27 = 26 + 1$.

مفتاح التشفير:	1	3	5	7	9	11	15	17	19	21	23	25
مفتاح فك التشفير:	1	9	21	15	3	19	7	23	11	5	17	25

الفصل الرابع

شفرات للكسر

(١) مقدمة

كانت الأمثلة التي ذكرناها في الفصل الثالث بسيطة للضرورة؛ حيث يسهُل كسر شفرة معظمها على الرغم من أن الوضع لم يكن كذلك وقت تصميمها. تتضمن عملية تحليل الشفرة عادة قدرًا كبيرًا من المحاولة والخطأ، وقد يسَّرت التطورات الحديثة في التكنولوجيا — خاصة في مجال الكمبيوتر — إجراء مثل هذه العمليات. من الأمثلة البارزة على نمط اعتراض يتضمن المحاولة والخطأ عملية البحث الشامل عن المفتاح التي ناقشناها في الفصل الثاني. تعتبر تجربة جميع المفاتيح في شفرة فيجنر في حال وجود كلمة مفتاح طويلة نسبيًّا — لنقُلْ ستة أحرف — عمليةً شاقة للغاية عند محاولة كتابة كل مفتاح يدويًّا في القرن السادس عشر. في المقابل، إذا توفَّر لدينا كمبيوتر يستطيع تجربة 10 آلاف كلمة مفتاح تتألف من ستة أحرف في الثانية، فسيستغرق الأمر أقل من يوم واحد.

قبل أن ننتقل من الأمثلة التاريخية التي ناقشناها في الفصل السابق إلى مناقشة أساليب التشفير الحديثة، من الجدير بالذكر مناقشة مفهوم الشفرة غير القابلة للكسر. كان كثيرٌ من مصممي الشفرات يدَّعون عدم قابلية أنظمة شفراتهم للكسر، وهو ما كان يُسْفر عادةً عن نتائج كارثية. نعرض الآن مثالَين تاريخيين شهيرين للاعتقاد الخاطئ بعدم قابلية شفرة للكسر، مثال يرجع إلى القرن السادس عشر وآخَر إلى الحرب العالمية الثانية.

كانت ماري ملكةُ اسكتلندا تستخدم شكلًا من أشكال شفرة الاستبدال البسيط في خطاباتها السرية في القرن السادس عشر. كانت مراسلاتها تحتوي على خططها للفرار

من السجن واغتيال إليزابيث ملكة إنجلترا لتتمكن من الاستيلاء على عرش إنجلترا. جرى اعتراض رسائل ماري، وفك شفرتها، واستخدامها كدليل في محاكمتها. ناقشت ماري والمتآمرون معها خططهم بكل صراحة في هذه الخطابات المشفَّرة؛ إذ استبعدوا قدرة أحد على قراءتها. كان ذلك خطأً كلَّف ماري حياتها.

استخدمت القوات الألمانية في الحرب العالمية الثانية جهازًا كان يُطلق عليه ماكينة إنيجما لتشفير معظم المراسلات العسكرية المهمة وغير المهمة. تبدو الآليات المستخدمة في ماكينة إنيجما للتشفير دقيقة ومعقدة؛ حيث كانت ماكينة إنيجما العادية تستخدم أكثر من 10^{20} مفاتيح، وهو ما يزيد عن بعض أنظمة الخوارزميات الحديثة. أدى ذلك إلى اعتقاد المستخدمين بأن شفرات إنيجما غير قابلة للكسر. كما هو معروف الآن، استطاعت قوات الحلفاء في أكثر من مناسبة حل شفرات ماكينات إنيجما الألمانية، عن طريق استغلال أخطاء الاستخدام وإدارة المفاتيح. تركَّزت جهود حل شفرات إنيجما في حديقة بلتشلي التي صارت متحفًا في الوقت الحالي. يرى البعض أن الجهود المبذولة في حديقة بلتشلي جعلت فترة الحرب العالمية الثانية أقصر بعامين.

في هذا الفصل، نناقش مفهوم السرية التامة التي تمثِّل — في معنًى من معانيها — أفضل ما يمكن أن نطمح إليه في التشفير. نناقش بعد ذلك دفتر المرة الواحدة، وهو الخوارزمية الوحيدة غير القابلة للكسر.

(٢) السرية التامة

يتمثل السيناريو العام الذي عرضناه حتى الآن في طرف مرسِل يحاول إرسال رسالة سرية إلى متلقٍّ محدد، ويستخدم نظام تشفير بحيث يجعل النص المشفَّر غير مفهوم بالنسبة إلى أي طرف ثالث. وحتى في حال فشل الطرف الثالث في اعتراض الرسالة، من الممكن، على الرغم من استحالة ذلك في معظم الحالات، تخمينُ محتوى الرسالة. من هنا، لا توجد طريقة يمكن من خلالها ضمان عدم حصول طرف ثالث على محتوى الرسالة عند استخدام التشفير. لا يملك الطرفان المتراسلان في حالِ نجاح طرف ثالث في اعتراض الرسائل بينهما سوى تمنِّي ألا تعطيه هذه المراسلات أيَّ معلومات عن محتوياتها. بعبارة أخرى، يجب أن يجري تصميم نظام التشفير بحيث لا يكون في وسع من يحصل على النص المشفَّر سوى تخمين محتوى الرسالة. لكنه لا توجد طريقة يمكن من خلالها منع الأطراف المعترضة من محاولة تخمين محتويات الرسائل.

يوفِّر النظام الذي ينجح في تحقيق هذا الهدف السرية التامة. نضرب الآن مثلًا صغيرًا لبيان أن تحقيق السرية التامة مسألة ممكنة.

هَبْ أن السيد س على وشك اتخاذ قرار سيكون له تداعيات خطيرة على قيمة الأسهم لإحدى الشركات؛ إذا اتخذ قرارًا «بالشراء» فسترتفع قيمة الأسهم، بينما إذا اتخذ قرارًا «بالبيع» فسيؤدي ذلك إلى انهيار قيمة الأسهم. هب أيضًا أن الجميع يعرف بأنه سرعان ما سيُصدر رسالة إما بالشراء أو بالبيع إلى وكيل أسهمه؛ بداهةً، كلُّ مَن يعرف قرار السيد س قبل وكيل أسهمه ستسنح له الفرصة لاستخدام هذه المعلومة لتحقيق الربح أو تفادي وقوع خسارة فادحة، وهو ما يعتمد على طبيعة القرار. بطبيعة الحال، في أي وقت من الأوقات، يستطيع الجميع تخمين نوع القرار والتصرف بناءً على ذلك. ويمتلك الجميع فرصةَ نجاح تبلغ ٥٠٪، وهو ما لا يعدو أكثر من عملية مقامرة.

يرغب السيد س في إرسال قراره عبر شبكة عامة فَوْرَ الاستقرار بشأنه. وهكذا، حتى يتمكن هو ووكيل أسهمه من حماية مصالحهما، يقرران تشفير الرسالة التي تنقل القرار. يتمثَّل أحد خيارات ذلك في استخدام نظام شفرات الاستبدال البسيط الذي، كما أشرنا سابقًا، يصلح لحماية الرسائل القصيرة. ومع ذلك في هذا المثال على وجه الخصوص، تُعرف كل رسالة من خلال طولها. من هنا، بافتراض معرفة الطرف المعترض بالنظام المستخدم في التشفير، ستكفي معرفة طول النص المشفَّر لمنح الطرف المعترض ثقة ١٠٠٪ في معرفة محتوى الرسالة، حتى وإن لم يستطع تحديد المفتاح المستخدم.

يتمثَّل أحد الخيارات الأخرى في استخدام النظام التالي؛ حيث يُحتمل استخدام المفتاحين k1 وk2 بنفس القدر. لوصف الخوارزمية كاملة سنستخدم رموزًا قياسية (عامة). بالنسبة إلى المفتاح k1، يتمثَّل النص المشفر لرسالة النص الأصلي BUY (شراء) في 0، بينما يتمثَّل النص المشفر لرسالة النص الأصلي SELL (بيع) في 1. للتعبير عن ذلك، نكتب $E_{k1}(BUY) = 0$، و$E_{k1}(SELL) = 1$. يجب قراءة الصيغة $E_{k1}(BUY) = 0$ كالآتي: «تتمثل نتيجة تشفير BUY باستخدام المفتاح k1 في 0.» والشفرة الكاملة تكون كما يلي:

$$\text{key k1: } E_{k1}\ (BUY) = 0,\ E_{k1}\ (SELL) = 1$$

$$\text{key k2: } E_{k2}\ (BUY) = 1,\ E_{k2}\ (SELL) = 0$$

هناك طريقة أخرى مكافئة لكتابة الشفرة نفسها يبينها الشكل التالي:

	BUY	SELL
Key k1	0	1
Key k2	1	0

إذا جرى استخدام هذا النظام، وجرى اعتراض الرقم 0، فإن كل ما على الطرف المعترض عمله هو استنباط أن الرسالة قد تكون SELL إذا استُخدم المفتاح k2، أو BUY حال استخدام المفتاح k1. وهكذا، سيضطر الطرف المعترض إلى تخمين أي مفتاح يجري استخدامه، وبما أن احتمال استخدام أيٍّ مِن المفتاحين يتساوى في الحالتين، تبلغ فرص تخمين الطرف المعترض للمفتاح على نحو صحيح ٥٠٪.

ثمة ملاحظة جوهرية؛ وهي أنه قبل اعتراض النص المشفَّر لم يتوفر لدى المعترض أي خيار سوى محاولة تخمين محتوى الرسالة. وبمجرد الاطلاع على النص المشفَّر، يستطيع الطرف المعترض تخمين المفتاح أيضًا. وبما أن عدد المفاتيح يساوي عدد الرسائل، تتساوى احتمالات صحة كلا التخمينين، وهو ما يعتبر نموذجًا للسرية التامة. بالنسبة إلى هذا المثال تحديدًا، تبلغ احتمالات تخمين الطرف المعترض للرسالة ٥٠٪، وهي نسبة مرتفعة. من هنا، على الرغم من وجود سرية تامة، لم تتوفر أي حماية إضافية لزيادة احتمال بقاء الرسالة سرية. ومع ذلك يرجع وجه القصور إلى أن عدد الرسائل صغير. إنه ليس ناتجًا عن عملية تشفير ضعيفة.

ثمة عدد من الحالات الواقعية يكون فيها عدد الرسائل المحتملة محدودًا للغاية، وهو ما يزيد من مخاطر تخمين محتوى الرسائل في هذه الحالات إذا ما قورنت بمخاطر فك شفرة الرسائل ذاتها. من الأمثلة التي تكاد تؤثر علينا جميعًا استخدامُ أرقام التعريف الشخصية وبطاقات الائتمان أو بطاقات ماكينات الصراف الآلي. في مثل هذه الحالة، يمتلك الأشخاص رقمَ تعريف شخصيًّا يحدد هويتهم كمالكين للبطاقات. إذا جرى التحقق من الرقم الشخصي من خلال كمبيوتر مركزي في إحدى المؤسسات المالية، فسيستخدم التشفير في حماية الرقم خلال انتقاله من ماكينة الصراف الآلي إلى الكمبيوتر المُضيف. فإذا فقد أحد المستخدمين بطاقاته، فسيستطيع أي شخص يعثر عليها إدخال

البطاقة في الماكينة وإدخال قيمةً «يخمنها» لرقم التعريف الشخصي. تتألف معظم أرقام التعريف الشخصية من أربعة أعداد (عشرية)؛ لذا هناك على الأكثر 10 آلاف قيمة لأرقام التعريف الشخصية. نظريًّا، يستطيع الشخص الذي يعثر على البطاقة إجراء العديد من محاولات تخمين الرقم الشخصي إلى أن يكتشف الرقم الصحيح، وهو ما يعتبر أسهل من كسر التشفير. بالإضافة إلى ذلك، لا يوجد حل تشفيري لهذه المشكلة. واعترافًا بهذه الحقيقة، لا تسمح معظم الأنظمة بأكثر من ثلاث محاولات لإدخال رقم تعريف شخصي خطأ قبل احتجاز البطاقة في ماكينة الصراف الآلي. يعتبر هذا المثال واحدًا من أمثلة عديدة لا يوفر التشفير فيها سوى حل جزئي؛ ومن ثَمَّ تصبح قرارات إدارة المفاتيح الخاصة بهذه الحالات ضرورية لزيادة أمن النظام.

من الجدير بالذكر ملاحظة أن الاتفاق، في مثالنا البسيط للسرية التامة، على استخدام مفتاح بعينه كان من الممكن التوصل إليه بمجرد معرفة طرفَي المراسلة بحاجتهما على الأرجح إلى تبادل بيانات سرية. كان من الممكن أن يحدث هذا الاتفاق في منزل أيٍّ مِن الطرفين، وكان من الممكن أن تتحقق سرية المفاتيح من خلال وسائل مادية مثل الاحتفاظ بها في خزانة آمنة إلى حين الحاجة إليها. تصبح هذه الملاحظة ذات أهمية خاصة عند قراءة موضوع إدارة المفاتيح في الفصل الثامن.

على الرغم من اشتمال المثال الذي طرحناه حول السرية التامة على رسالتين فقط، من الممكن تصميم أنظمة مشابهة لأي عدد من الرسائل. ومع ذلك لا يمكن تحقيق السرية التامة إلا عند تَساوي عدد المفاتيح على الأقل مع عدد الرسائل.

(٣) دفتر المرة الواحدة

تتمثل إحدى النتائج الأساسية المترتبة على مناقشتنا للسرية التامة في إمكانية تحقيقها، ولكن في حالة الأنظمة التي تشتمل على عدد هائل من الرسائل المحتملة لا يتحقق هذا إلا على حساب ارتفاع تكلفة الإدارة الفعالة لعدد هائل من المفاتيح. والمثال الكلاسيكي على نظام تشفير آمن تمامًا هو نظام «دفتر المرة الواحدة». فإذا كانت الرسالة عبارة عن فقرة من نص إنجليزي يحتوي على عدد n من الأحرف مع التخلص من جميع علامات الترقيم والمسافات، يكون المفتاح — الذي يستخدم مرة واحدة فقط لحماية رسالة واحدة — عبارة عن سلسلة مكونة من n حرفًا هجائيًّا مولدة عشوائيًّا. وتعتبر قاعدة التشفير هنا هي نفس القاعدة المستخدمة في شفرة فيجنر مع الاستعاضة عن كلمة المفتاح بالمفتاح.

من هنا، إذا ربطنا بين كل حرف من A إلى Z والأعداد من 0 إلى 25 بالطريقة المعتادة، للرسائل $m_1, m_2, \ldots, m_n$ والمفاتيح $K_1, K_2, \ldots, K_n$، نحصل على الحرف رقم i في النص المشفَّر من خلال الصيغة التالية:

$$C_i = (m_i + K_i) \bmod 26$$

(مقياس حسابي = mod 26)

لاحظ أنَّ تَساوي طول الرسالة مع المفتاح يضمن عدم الحاجة إلى البدء في تكرار المفتاح خلال عملية التشفير.

ثمة نسخة أخرى شائعة من هذه الخوارزمية يطلق عليها «شفرة فرنام» التي تَكُون الأحرف المستخدمة فيها ثنائية؛ أي 0 و1، كما يجري الحصول على النص المشفَّر من خلال جمع الرسالة والمفتاح للمقياس الحسابي 2. بالنسبة إلى الاتصالات الرقمية، تعتبر شفرة فرنام هي نسخة دفتر المرة الواحدة التي يجري استخدامها.

بما أن السرية التامة قابلة للتحقق، قد يسأل المرء: لماذا لا يستعين بها الجميع على نطاق واسع؟ ولماذا يستخدم الناس أنظمة يمكن كسر شفراتها؟ قبل الإشارة إلى أي إجابة لأسئلة من هذا النوع، من الأهمية بمكان تذكُّر أن المشكلات المصاحبة لاستخدام التشفير في حالة البيانات المخزنة تختلف عن تلك المشكلات المصاحبة لاستخدام التشفير لحماية الاتصالات. كذلك من الأهمية بمكان تذكر أننا عادة ما نركِّز على الاتصالات؛ نظرًا لأنها تشكِّل مشكلات إدارية أكثر من غيرها.

عند تعريف نظام دفتر المرة الواحدة، اقتصرنا في الحديث على ذكر خوارزمية التشفير ومفتاح التشفير. يتطابق مفتاح فك التشفير مع مفتاح التشفير في حين تتضمن خوارزمية فك التشفير طرح المفتاح من النص المشفَّر للحصول على النص الأصلي. قد يواجه منفذو أنظمة الاتصالات حاليًّا مشكلة صعبة؛ وهي كيف يحصل المستقبِل على هذه السلسلة المتتالية العشوائية؟ فبما أن هذه السلسلة مولدة عشوائيًّا، يعد من قبيل «المستحيل» بالنسبة إلى المرسل والمستقبل توليد المفتاح نفسه آنيًّا؛ لذا، يجب على أحدهما توليد المفتاح ثم إرساله (سريًّا) إلى الطرف الآخر. ولضمان سرية تبادل المفتاح، يجب توفير الحماية له خلال عملية الانتقال. فإذا كانت الأطراف المتراسلة لديها قناة اتصال واحدة فقط، فإنها ستحتاج إلى سلسلة عشوائية أخرى لنظام دفتر المرة الواحدة لحماية السلسلة الأولى. بداهةً، يفضي ذلك إلى مجموعة لا نهائية من السلاسل العشوائية،

يُستخدم كلٌّ منها في حماية السلسلة السابقة عليها خلال نقلها من طرف إلى آخر. من هنا، تُستخدم دفاتر المرة الواحدة فقط في حال امتلاك الأطراف المتراسلة وسيلةً ثانية آمنة لتبادل المعلومات. ربما يتذكر القارئ أن السيد س ووكيل أسهمه كانا لديهما مثل هذه الوسيلة في المثال الذي عرضناه عن نظام السرية التامة. ويرى البعض أيضًا أن دفاتر المرة الواحدة تُستخدم في أعلى مستويات روابط الاتصال الآمنة، مثل خطوط الاتصال الساخنة بين موسكو وواشنطن. في هذه الحالات، عدد من السلاسل العشوائية يمكن توليدها وتخزينها، ثم حملها إلى مواقع أخرى من خلال خدمات البريد السريع الآمن. يمكن بعد ذلك تخزين السلاسل العشوائية في مواقع تتمتع بمستويات حماية مرتفعة ولا يجري استرجاعها إلا عند الطلب، ويجري تدميرها بعد استخدامها مباشرةً. من الأهمية بمكان إدراك أن هذه القناة الآمنة الثانية تتصف بالبطء وارتفاع التكلفة؛ ومن ثَمَّ لا يمكن استخدامها في تبادل الرسائل؛ حيث قد تكون الردود والاستجابات الفورية مطلوبة.

مثلما أشرنا، لا تقتصر مشكلة توزيع المفاتيح عبر شبكة آمنة على دفتر المرة الواحدة فقط؛ فالحاجة إلى قناة آمنة ثانية مسألة شائعة. يتمثل الفرق بين الحالتين في أنه بينما يتساوى حجم المحتوى في الرسائل المتبادَلة مع حجم الرسائل نفسها في دفتر المرة الواحدة، تحمل القناة الآمنة الثانية عددًا أقل من الرسائل المتبادلة. حتى في حال استخدام رابط آمن ثانٍ، لا يعتبر دفتر المرة الواحدة مناسبًا بالنسبة للأنظمة التي تشتمل على العديد من نقط الاتصال التي يحتاج كلٌّ منها إلى رابط آمن مع غيرها من نقط الاتصال. والمشكلة هنا هي تتبع المفاتيح المستخدمة، وربما التعامل مع الحجم الهائل لمحتويات المفاتيح. وحيث إن السرية التامة تقوم على استخدام كل مفتاح مرة واحدة، فإن حجمَ محتويات المفاتيح المطلوبة لشبكة كبيرة كثيفة الاستخدام سيجعل عمليةَ إدارة المفاتيح مسألةً غير قابلة للتطبيق مطلقًا.

لا عجب أنه على الرغم من أن دفتر المرة الواحدة يوفر أقصى مستويات الحماية، لا توجد سوى شبكات اتصالات محدودة للغاية تستعين بها. بطبيعة الحال، إذا كان يجري تشفير الملفات استعدادًا لتخزينها للاستخدام الشخصي، فلن تبرز الحاجة إلى توزيع أي مفاتيح. وفي كثير من حالات التخزين، تتعلق المشكلات الرئيسية بتخزين المفاتيح؛ ومن ثَمَّ، في بعض هذه الحالات ربما تَصلح دفاتر المرة الواحدة لحماية الملفات مثلها مثل أي شفرة أخرى.

الفصل الخامس

الخوارزميات الحديثة

(١) مقدمة

خلال الفصل الثالث، أكَّدْنا على أن الأمثلة التي عرضناها لا تشير إلى الممارسات الحالية، وأن نظام خوارزميات التشفير الحديثة تَستخدم في الأغلب البتات (الأرقام الثنائية) بدلًا من استبدال الأحرف في الأمثلة التي عرضناها. في هذا الفصل، نناقش الخوارزميات الحديثة. وبما أنها أكثر تعقيدًا من أمثلة الخوارزميات التي سقناها في الفصل الثالث، فإننا لا نذكر أيَّ أمثلة محددة بالتفصيل، لكننا نركِّز على الأساليب العامة المستخدمة في تصميمها.

(٢) سلاسل الرقم الثنائي (البت)

مثلما أشرنا سابقًا، لا تتضمن الشفرات الحديثة عملية استبدال للأحرف. بدلًا من ذلك، عادة ما يَستخدم التشفير الحديث أنظمة ترميز لتحويل الرسائل إلى سلسلة متتالية من الأرقام الثنائية (بتات)؛ أي من أصفار وآحاد. ويعد نظام إيه إس سي آي آي (نظام الترميز القياسي الأمريكي لتبادل المعلومات، آسكي) على الأرجح أكثر أنظمة التشفير الحديثة شيوعًا. بعد ذلك، يجري تشفير سلسلة الأرقام الثنائية هذه التي تمثِّل النص الأصلي للحصول على النص المشفر في صورة سلسلة الأرقام الثنائية.

يمكن تطبيق خوارزمية التشفير على سلسلة الأرقام الثنائية بطرق عدة. ثمة فارق «طبيعي» بين نظام «شفرات التدفق»؛ حيث يتم تشفير السلسلة بتًّا بتًّا (أي رقمًا ثنائيًّا رقمًا ثنائيًّا)، ونظام «شفرات الكتل»؛ حيث يتم تقسيم السلسلة إلى كتل (مجموعات) لها طول مُحدد سلفًا. يتطلب نظام الترميز القياسي الأمريكي لتبادل المعلومات ثَمانية بتات

لتمثيل رمز واحد؛ لذا، يُجرى تطبيق خوارزمية التشفير على ثمانية رموز مرة واحدة في حالة شفرة الكتل التي تكون فيها الكتلة تتألف من 64 رقمًا ثنائيًّا.

من الأهمية بمكان أن ندرك أن سلسلة الأرقام الثنائية نفسها يمكن كتابتها بطرق مختلفة، كما يتعين علينا أن ندرك أن طريقة كتابتها تعتمد على طول الكتل التي جرى تقسيمها إليها.

خذ — على سبيل المثال — السلسلة التالية المؤلفة من 12 رقمًا ثنائيًّا: 11 01 10 10 01 01. إذا قسمنا هذه السلسلة إلى كتل تتألف من ثلاثة أرقام ثنائية نحصل على: 110 010 111 100. في المقابل، أيُّ سلسلة أرقام ثنائية بطول 3 تمثل عددًا صحيحًا يقع بين قيمتَيْ 0 و7؛ ومن ثَمَّ تتخذ السلسلة التي لدينا الصورة الآتية: 6 2 7 4. بالنسبة إلى هؤلاء ممن لم يقرءوا الملحق في الفصل الثالث ولا يمتلكون معرفة كافية بطرق التمثيل الثنائي للأعداد الصحيحة، تكون السلسلة على النحو التالي:

000 = 0, 001 = 1, 010 = 2, 011 = 3, 100 = 4, 101 = 5, 110 = 6, 111 = 7.

إذا أخذنا السلسلة نفسها ثم قسمناها إلى كتلٍ بطول أربعة نحصل على: 0110 1101 1001. في هذه المرة، بما أن سلسلة الأرقام الثنائية التي لها طول أربعة أرقام ثنائية تمثِّل الأعداد الصحيحة الواقعة بين قيمتَيْ 0 و15، نحصل على السلسلة 9136. بوجه عام، يمكن النظر إلى سلسلة الأرقام التي طولها N على أنها تمثِّل عددًا صحيحًا يقع بين قيمتَيْ 0 و$2^N - 1$؛ ومن ثَمَّ، بمجرد الاتفاق على طول كتلة بقيمة S، يمكن كتابة أي سلسلةِ أرقام ثنائية طويلة كسلسلةٍ تتألف من أعداد صحيحة تقع في نطاق القيمتين 0 و$2^S - 1$.

بينما لا تعتبر التفاصيل الرياضية الدقيقة مهمة، من الأهمية بمكان ملاحظةُ أن سلسلة الأرقام الثنائية نفسها يمكن تمثيلها في صورة سلسلة من الأعداد بعدة طرق، اعتمادًا على طول الكتلة التي جرى انتقاؤها. من الأهمية بمكان أيضًا إدراك أنه في حال تحديد طول الكتلة، وكانت الأعداد صغيرة، ربما يكون ضروريًّا إضافة بعض الأصفار الإضافية في البداية. على سبيل المثال، يعتبر التمثيل الثنائي للعدد الصحيح 5 هو 101. في المقابل، في حال استخدام كتلة طولها 6 أعداد تمثِّل 5 كالآتي: 000101، وبالنسبة إلى كتلة طولها 8، فإننا نمثل 5 كالآتي: 00000101.

هناك طريقة أخرى شائعة لكتابة سلسلة الأرقام الثنائية؛ وتتمثل في استخدام «التمثيل السادس العشر». بالنسبة إلى التمثيل السادس عشر، تُقسَّم السلسلة إلى مجموعات من أربعة أعداد تمثَّل كالآتي:

0000 = 0	0001 = 1	0010 = 2	0011 = 3
0100 = 4	0101 = 5	0110 = 6	0111 = 7
1000 = 8	1001 = 9	1010 = A	1011 = B
1100 = C	1101 = D	1110 = E	1111 = F

من هنا، يصير التمثيل السادس عشر للسلسلة السابقة: 6 D 9.

بما أن خوارزميات التشفير يجري تطبيقها على سلسلة من الأرقام الثنائية فسنحتاج إلى التعرف على أسلوبٍ شائعِ الاستخدام لدمج رقمين ثنائيين يطلق عليه أسلوب «أُو آر الحصري» وعادةً ما يجري كتابته كالآتي: «إكس أو آر» أو $\oplus$. إنه يطابق الجمع بالنسبة إلى المقياس الحسابي 2 ويعرَّف كالآتي: $0 \oplus 0 = 0$، $0 \oplus 1 = 1$، $1 \oplus 0 = 1$، و$1 \oplus 1 = 0$، وهو ما يمكن تمثيله في جدول.

	0	1
0	0	1
1	1	0

جدول عملية إكس أو آر أو $\oplus$.

توفر هذه العملية البسيطة طريقة للدمج بين سلسلتين من الأرقام الثنائية لهما نفس الطول. نجري هذه العملية على أزواج من الأرقام الثنائية في مواضع متناظرة. على سبيل المثال، هب أننا نريد حساب $10011 \oplus 11001$. الرقم الثنائي إلى يسار 10011 هو 1 والرقم الثنائي إلى يسار 11001 هو 1 أيضًا؛ من هنا، بما أن الرقم الثنائي إلى يسار $10011 \oplus 11001$ يجري الحصول عليه من خلال تطبيق أسلوب إكس أو آر على الأرقام الثنائية في يسار كل سلسلة منفردة، نجد أن الرقم الثنائي إلى

$10011 \oplus 11001$ هو $1 \oplus 1$، والذي هو 0. بمواصلة إجراء العملية نفسها نحصل على: $10011 \oplus 11001 = 1 \oplus 10 \oplus 10 \oplus 01 \oplus 01 \oplus 1 = 01010$. يبين الشكل التالي طريقة أخرى لكتابة العملية الحسابية:

$$\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ \hline 1 \oplus 1 & 0 \oplus 1 & 0 \oplus 0 & 1 \oplus 0 & 1 \oplus 1 \\ 0 & 1 & 0 & 1 & 0 \end{array}$$

(٣) شفرات التدفق

يستخدم الكثير من المؤلفين هذا المصطلح بطريقة مختلفة نوعًا ما. يتحدث الكثيرون عن شفرات تدفق تعتمد على الكلمات أو الرموز. في هذه الحالة يجري تشفير الرسالة كلمة كلمة (أو رمزًا رمزًا)، ويجري تحديد قاعدة التشفير لكل كلمة (رمز) من خلال موضعها في الرسالة. تتوافق شفرة فيجنر، التي جرى مناقشتها في الفصل الثالث، ودفتر المرة الواحدة مع هذا التعريف. ربما كان أكثر النماذج التاريخية شهرةً هو شفرة إنيجما. في المقابل، يتمثَّل أكثر الاستخدامات الحديثة شيوعًا لمصطلح «شفرة تدفق» — وهو الاستخدام الذي نتبناه هنا — في أنها شفرة يجري تشفير النص الأصلي فيها رقمًا رقمًا. بداهةً، كل ما يمكن أن يحدث لأي رقم ثنائي هو تغيُّر قيمته إلى القيمة البديلة أو عدم تغيرها. وبما أن أي رقم ثنائي يمكن أن يكون له قيمة واحدة من قيمتين اثنتين فقط، فإن تغيير أي رقم ثنائي يعني تبديله بقيمة أخرى. بالإضافة إلى ذلك، إذا جرى تغيير رقم ثنائي مرتين، فإنه يعود إلى قيمته الأصلية.

إذا كان الطرف المعترض يعلم أن شفرة تدفق جرى استخدامها، فسينحصر جهده إذنْ في تحديد مواضع الأرقام الثنائية التي جرى تغييرها، ثم تغييرها إلى قيمها الأصلية. إذا كان ثمة نمط سهل التتبع يمكن من خلاله تحديد الأرقام التي جرى تغييرها، فربما ستصبح مهمة الطرف المعترض سهلة. من هنا، بينما يجب ألا تكون مواضع الأرقام الثنائية التي جرى تغييرها قابلة للتنبؤ من قبل الطرف المعترض، بل يجب أن يتمكن الطرف المستقبل دومًا من تحديدها بسهولة.

بالنسبة إلى شفرات التدفق، يجري النظر إلى عملية التشفير باعتبارها سلسلة تتألف من العمليتين الآتيتين: التغيير وعدم التغيير. يحدد مفتاح التشفير هذه السلسلة التي

عادة ما يطلق عليها سلسلة «مفتاح التدفق». للتبسيط والاختصار، لنتفقْ على أن قيمة 0 تشير إلى «عدم التغيير» وقيمة 1 تشير إلى «التغيير». بلغْنا الآن مرحلةً صار فيها النص الأصلي، والنص المشفر، ومفتاح التدفق كلها سلاسلَ تتألف من أرقام ثنائية.

للمزيد من التوضيح، هب أن لدينا النص الأصلي 1100101 ومفتاح التدفق 1000110؛ إذن، بما أن قيمة 1 في مفتاح التدفق تشير إلى تغيير الرقم الثنائي في النص الأصلي في ذلك الموضع، فسنجد أن قيمة 1 التي تقع في أقصى يسار النص الأصلي يجب تغييرها، لكننا سنلاحظ أن الرقم الثنائي التالي يظل كما هو. بتكرار هذه العملية نحصل على النص المشفر 0100011. أشرنا توًّا إلى أن تغيير رقم ثنائي مرتين يترتب عليه إعادة الرقم إلى قيمته الأصلية؛ وهو ما يعني أن عملية فك التشفير تماثل عملية التشفير؛ ومن ثَمَّ يحدد مفتاح التدفق أيضًا طريقة فك التشفير.

يتمثَّل كل ما قمنا به في العرض السابق في «دمج» سلسلتين من الأرقام الثنائية لتوليد سلسلة ثالثة من خلال قاعدة يمكن النص عليها كالآتي في حالتنا الخاصة هذه: «إذا كان هناك رقم 1 في أحد مواضع السلسلة الثانية، غيِّر إذن الرقم في الموضع نفسه من السلسلة الأولى.» تعتبر هذه العملية هي بالضبط عملية إكس أو آر، أَو التي سبق تعريفها في الجزء السابق. من هنا إذا كانت كلٌّ مِن P_i، K_i وC_i تمثِّل الرقم الثنائي للنص الأصلي، ومفتاح التدفق، والنص المشفر على التوالي في الموضع i، يجري الحصول على الرقم الثنائي للنص المشفر C_i من خلال $C_i = P_i \oplus K_i$. لاحظ أن عملية التشفير تُعرف من خلال $P_i = C_i \oplus K_i$.

تعتبر شفرات التدفق أحد التنويعات العملية الأساسية لشفرة فرنام باستخدام مفاتيح صغيرة. تتمثل المشكلة في دفتر المرة الواحدة في أنه بما أن مفتاح التدفق يكون عشوائيًّا، فمن المستحيل توليد نفس مفتاح التدفق آنيًّا على طرفَي الإرسال والاستقبال، وهو ما يجعلها تتطلب قناة ثانية آمنة لتوزيع المفاتيح، وهذه القناة تحمل من المحتوى ما يساوي محتوى قناة الاتصالات الرئيسية. وتجري نفس الاشتراطات في حالة شفرات التدفق مثلما هو الحال مع أي قناة آمنة للمفتاح، ولكن في ظل وجود محتوى معلومات أقل بكثير.

تحتاج شفرة التدفق إلى مفتاح قصير لتوليد مفتاح تدفق طويل، وهو ما يتحقق من خلال استخدام مولِّد سلسلة أرقام ثنائية. تذكَّرْ أننا خلال مناقشتنا لشفرة فيجنر في الفصل الثالث، طرحنا مفهوم استخدام مولِّدٍ لتوليد مفتاح تدفق طويل ذي أحرف

هجائية من خلال مفتاح قصير ذي أحرف هجائية. لكن في تلك الحالة، كانت عملية التوليد بدائية للغاية؛ إذ جرى انتقاء كلمة المفتاح وتكرارها. يجب أن تكون مولدات مفتاح التدفق في شفرات التدفق العملية أكثر تعقيدًا من ذلك. للتدليل على سبب ذلك، نلاحظ مما سبق أن الرقم الثنائي لمفتاح التدفق في الموضع i، $K_i = P_i \oplus C_i$ يمكن تحديده على أنه نتاج عملية إكس أو آر للنص الأصلي والنص المشفر في الموضع i. يسلط ذلك الضوء على ضعف شفرات التدفق؛ حيث إن أي طرف معترض يتمكن من إجراء عملية اعتراض استنادًا إلى معرفته بالنص الأصلي سيستطيع استنباط أجزاء من سلسلة مفتاح التدفق من خلال زوجَي الأرقام الثنائية للنص الأصلي والنص المشفر المقابلين. من هنا، يجب على مستخدمي شفرات التدفق حماية شفراتهم ضد عمليات الاعتراض التي يستطيع الطرف المعترض عبرها استنباط جزء من مفتاح التدفق. بعبارة أخرى، يجب أن تكون سلسلة مفتاح التدفق غير متوقعة؛ بمعنى أن القدرة على معرفة جزء منها يجب ألا يمكِّن الطرف المعترض من استنباط الباقي. على سبيل المثال، تنتج شفرةُ فيجنر التي لها مفتاح قصير بطول 4 مفتاحَ تدفُّقٍ يتكرر كل أربعة رموز. ومع ذلك من السهولة بمكان تصميم مولدات مفاتيح تدفُّق تتكرر كل خمسة عشر رقمًا ثنائيًّا، وذلك بانتقاء مفتاح مكون من أربعة أرقام ثنائية. لتنفيذ ذلك، نبدأ بأي مفتاح يبلغ طوله أربعة أرقام فيما عدا 0000. تُجرى عملية توليد — على سبيل المثال — بالحصول على كل رقم ثنائي من السلسلة الرقمية عن طريق إجراء عملية إكس أو آر للرقمين الثنائيين الأول والأخير للأرقام الثنائية الأربعة التي تسبقها. إذا بدأنا برقم 1111 تصبح السلسلة 111101011001000، ثم تتكرر إلى ما لا نهاية. في حقيقة الأمر، يمكن إجراء عملية التوليد مباشرةً من خلال انتقاء مفتاح طوله n، ثم توليد مفتاح تدفُّق لا يبدأ في التكرار إلا عند بلوغ $2^N - 1$ رقم ثنائي.

تعتبر عملية تصميم مولدات لسلسلة مفتاح تدفق جيدة عملية في غاية الصعوبة، وهو ما يتطلب معرفة بمستوًى متقدم من الرياضيات. بالإضافة إلى ذلك، هناك حاجة إلى إجراء اختبارات إحصائية مكثفة لنضمن — إن أمكن — أن ناتج المولد لا يمكن تمييزه عن سلسلة عشوائية. على الرغم من ذلك، يوجد عدد من التطبيقات تُعتبر شفرات التدفق هي الأكثر ملائمة لها. يتمثل أحد أسباب ذلك في أنه في حال تلقِّي رقم ثنائي في النص المشفر على نحو غير صحيح، فإنه سيكون هناك رقم ثنائي واحد فقط في فك الشفرة غير صحيح؛ حيث يقابل كلَّ عدد ثنائي في النص الأصلي رقمٌ ثنائي واحد فقط

في النص المشفر. لا ينطبق ذلك على شفرات الكتل؛ حيث يؤدي تلقِّي رقم واحد فقط غير صحيح في النص المشفر إلى عدم مصداقية الكتلة بعد فك تشفيرها. عدم «انتشار الخطأ» هذا عن طريق خوارزمية فك التشفير أمر ضروري إذا كان يجري نقل النص المشفر عبر قناة مشوشة؛ ومن ثَمَّ، تُستخدم شفرات التدفق في تشفير الأحاديث الممثلة رقميًّا مثل شبكات الهواتف المحمول بنظام جي إس إم. المميزات الأخرى لشفرات التدفق التي تتميز بها عن شفرات الكتل تشمل السرعة وسهولة التنفيذ.

(٤) نظام شفرات الكتل (نمط كتاب الشفرات الإلكتروني)

في حالة «شفرة الكتل»، يتم تقسيم سلسلة الأرقام الثنائية إلى كتل أو مجموعات بطول محدد. تطبَّق خوارزمية التشفير على هذه الكتل لتوليد كتل نص مشفَّر لها نفس الطول وذلك في حال معظم الشفرات المتناظرة.

هناك العديد من التطبيقات لشفرات الكتل. ويمكن الاستعانة بها لتوفير السرية، أو سلامة البيانات، أو التحقق من هوية المستخدمين، بل يمكن استخدامها في توفير مولد مفتاح التدفق في شفرات التدفق. ومثلما هو الحال مع شفرات التدفق، من الصعوبة بمكان إجراء عملية تقييم محددة لدرجة الأمن التي يحققها هذا النظام. بداهةً، مثلما رأينا، يمثِّل طول المفتاح حدًّا علويًّا لقوة خوارزمية التشفير. لكن مثلما رأينا في حالة نظام شفرات الاستبدال البسيط، لا يمثِّل توفر عدد كبير من المفاتيح ضمانة لقوة الشفرة. ويقال إن الخوارزمية المتناظرة «مصممة جيدًا» في حال ما إذا كانت عملية البحث الشاملة هي أبسط صور الاعتراض. بطبيعة الحال، يمكن أن تكون الخوارزمية مصممة جيدًا لكنها سهلة الكسر إذا كان عدد المفاتيح صغيرًا جدًّا.

يعتبر تصميم خوارزميات تشفير قوية مهارةً متخصصة. بيد أنه ثمة عدد من الخواص البديهية يجب أن تتوفر في شفرة الكتل القوية، وهي خواص يسهُل بيانها. إذا حصل طرف معترض على زوج من نص أصلي معروف ونص مشفر لمفتاح غير معروف، فلن يمكِّنه ذلك بالضرورة من استنباط النص المشفر المقابل لأي نص أصلي آخر. على سبيل المثال، لا تمتلك الخوارزمية التي يتغير فيها النص الأصلي بطريقة معروفة بحيث يؤدي إلى إحداث تغيير متوقع في النص المشفر، مثل هذه الخاصية. يمثل ذلك أحد أسباب اشتراط توفر «خاصية الانتشار» في نظام شفرات الكتل، وهي الخاصية التي تتمثل في

أن إجراء أي تغيير بسيط في النص الأصلي، ربما — على سبيل المثال — من خلال تغيير موضع أو موضعين، سيؤدي إلى حدوث تغيير غير متوقع في النص المشفر.

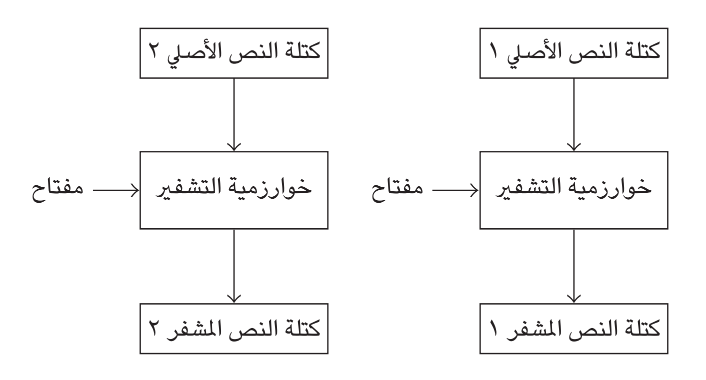
ناقَشْنا من قبل مخاطر عمليات البحث الشاملة للمفتاح. خلال إجراء مثل هذا النوع من عمليات البحث، قد يجرِّب الطرف المعترض مفتاحًا لا يختلف عن القيمة الصحيحة للمفتاح الحقيقي إلا في عدد محدود من المواضع. إذا كان ثمة دليل على أن الطرف المعترض جرَّب — على سبيل المثال — مفتاحًا لا يتفق مع المفتاح الصحيح في موضع واحد فقط، فقد يوقف الطرف المعترض عملية البحث ثم يكتفي بتغيير كل موضع لهذا المفتاح الخطأ على التوالي، وهو ما سيقلل كثيرًا من الوقت اللازم لاكتشاف المفتاح، وهذا أمر آخر غير مرغوب فيه. بناءً عليه، يجب أن تتوفر في شفرات الكتل «خاصية التشويش» التي تتمثل في أنه في حال محاولة طرف معترض إجراء عملية بحث شاملة عن المفتاح، يجب ألا تتوفر أي إشارة إلى «الاقتراب» من المفتاح الصحيح.

عند مناقشة شفرة الاستبدال البسيط، أعطَيْنا مثالًا على عملية اعتراض جرى فيها بناءُ مفتاح التشفير تدريجيًّا من خلال، أولًا، العثور على بديل الحرف **E**، ثم العثور على بديل الحرف **T**، وهكذا. إذا تمكن طرف معترض من تحديد أجزاء من المفتاح بطريقة مستقلة عن الأجزاء الأخرى، فسيُعد ذلك اعتراضًا من قبيل فَرِّقْ تَسُدْ. للحيلولة دون ذلك، يُشترط تحقيق «التكامل»؛ وهو ما يعني أن يعتمد كل رقم ثنائي في النص المشفر على كل رقم ثنائي في المفتاح.

تشكِّل عملية الاختبار الإحصائي مكونًا أساسيًّا لتقييم شفرات الكتل فيما يتعلق بهذه الخواص الثلاث، فضلًا عن خواص أخرى، وهو ما يجعل من الاختبار الإحصائي أمرًا ضروريًّا لتحليل الشفرات المتناظرة.

تتمثل أسهل الطرق، وربما أكثرها منطقية، لتشفير رسالة طويلة بشفرة الكتل في تقسيم سلسلة الأرقام الثنائية إلى كتل مناسبة الطول، ثم تشفير كل كتلة على حدة وعلى نحو مستقل. عندما يجري تنفيذ ذلك، نطلق على هذه العملية استخدام نمط «كتاب الشفرات الإلكتروني». عند انتقاء مفتاح واستخدام نمط كتاب الشفرات الإلكتروني، ينتج عن الكتل المتناظرة في الرسالة كتل متناظرة في النص المشفَّر؛ وهو ما يعني أنه في حال حصول طرف معترض على الزوج المقابل من كتلة النص الأصلي ونص التشفير، سيستطيع تحديد موضع الكتلة في النص الأصلي في كل مكان في الرسالة من خلال إيجاد الأرقام الثنائية المقابلة في النص المشفر. يعتبر شيئًا مفيدًا للغاية إذن بالنسبة إلى الطرف

المعترض أن يبدأ في بناء قاموس للكتل المقابلة المعروفة في النص الأصلي والنص المشفر. بالإضافة إلى ذلك، إذا كان ثمة كتل رسائل معروفة على نطاق واسع، فسيؤدي ذلك إلى ظهور كتل معروفة على نطاق واسع أيضًا في النص المشفَّر، وهو ما قد يؤدي إلى وقوع عملية الاعتراض نفسها القائمة على نمط التكرار التي استخدمناها في شفرات الاستبدال البسيط. يعتبر ذلك أحد دوافع انتقاء كتل كبيرة الطول نسبيًّا، مثل الكتل التي تشمل 64 رقمًا ثنائيًّا، تحتوي كل مجموعة منها على ثمانية رموز. ومع ذلك يوجد عيب محتمل في استخدام نمط كتاب الشفرات الإلكتروني، وهو ما سنبيِّنه من خلال مثال.



شفرات الكتل وفق نمط كتاب الشفرات الإلكتروني.

هَبْ أن شفرة كتل غير معروفة ومفتاحًا غير معروف جرى استخدامهما لتشفير الرسالة التالية: The price is four thousand pounds (السعر أربعة آلاف جنيه)؛ لا توجد معلومات متوفرة سوى أن كتلة من كتل الرسالة تتألف من حرفين، وأنه حدث تجاهل لعلامات الترقيم، والمسافات، إلخ، وأن النص المشفَّر على النحو التالي:

$$C_1,\ C_2,\ C_3,\ C_4,\ C_5,\ C_6,\ C_7,\ C_8,\ C_9,\ C_{10},\ C_{11},\ C_{12},\ C_{13},\ C_{14}.$$

هَبْ أن الطرف المعترض يعرف محتوى الرسالة؛ سيستطيع إذن استنباط أن C_1 تمثِّل TH، وأن C_2 تمثل ep، إلى آخره. ثم يتلاعب الطرف المعترض بالنص المشفَّر بحيث لا يجري تلقي سوى الكتل التالية: $C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_{12}, C_{13}, C_{14}$. ويستخدم الطرف المستقبل خوارزمية فك التشفير من خلال المفتاح الصحيح في فك

شفرة النص المشفَّر الذي يتلقاه ليحصل على الآتي: The price is four pounds (السعر أربعة جنيهات). بما أن عملية فك التشفير نجحت وصار للرسالة معنًى، فلن يشك الطرف المتلقي في أن النص المشفَّر جرى التلاعب به؛ ومن ثَمَّ سيفترض صحة السعر.

يمكن التخلص من هذه المخاطر المحتملة في استخدام شفرة الكتل وفق نمط كتاب الشفرات الإلكتروني من خلال جعل عملية التشفير لكل كتلة مفردة على حدة تعتمد على جميع الكتل التي تسبقها في الرسالة. في حال تنفيذ ذلك، فإن الكتل المتشابهة في الرسالة ستعطي على نحو شبه مؤكد كتلًا متشابهة في النص المشفَّر، وسيؤدي التلاعب في النص المشفَّر إلى رسائل لا معنَى لها بعد إجراء عملية فك التشفير. ثمة طريقتان قياسيتان لتحقيق ذلك؛ ألا وهما، نمط «استجابة الشفرات» ونمط «تسلسل شفرات الكتل»، اللذان يجري الحديث عنهما لاحقًا.

نذكر مثالًا بسيطًا لبيان طريقة عمل شفرات الكتل وفق نمط كتاب الشفرات الإلكتروني. الخوارزمية المستخدمة هنا ضعيفة. في المثال الذي نذكره، يبلغ طول كتل النص الأصلي، وكتل نص التشفير، والمفاتيح جميعها 4 أرقام ثنائية. نستخدم التمثيل السادس عشر للتعبير عن الكتل. بالنسبة إلى المفتاح K، يجري الحصول على كتلة النص المشفر **C** المقابلة لكتلة النص الأصلي M من خلال إجراء عملية إكس أو آر على M مع K ثم إجراء عملية تدوير للأرقام الثنائية لناتج $M \oplus K$ موضعًا واحدًا إلى اليسار.

نشفر سلسلة الأرقام الثنائية للنص الأصلي:

$$10100010001110101001$$

التي تصبح A23A9 عند استخدام أسلوب التمثيل السادس عشر مع مفتاح K = B. وتتم عملية التشفير على النحو التالي:

تذكر أننا نستخدم التمثيل السادس عشر؛ لذا، بالنسبة للكتلة الأولى M = 1010 وK = 1011؛ ومن ثَمَّ، $M \oplus K = 1001$. إذا أجرينا الآن عملية التدوير فسنجد أن كتلة النص المشفر هي 0010، التي تساوي 2 وفق التمثيل السادس عشر.

كذلك الحال بالنسبة للكتلة الثانية، في حال M = 2 وK = B؛ ومن ثَمَّ، M = 0010، K = 1001؛ ومن ثَمَّ $M \oplus K = 1011$. إذا أجرينا الآن عملية التدوير على رقم 1001، فسنجد أن كتلة النص المشفر تساوي 3 وفق التمثيل السادس عشر.

مع تكرار هذه العملية الحسابية نجد أن الرسالة هي A23A9 ومع استخدام شفرتنا وفق نمط كتاب الشفرات الإلكتروني في حال K = B، يكون النص المشفَّر هو 23124.

تتمثل الملاحظة البديهية هنا في أن الكتل المتكررة في الرسالة تؤدي إلى كتل متكررة في النص المشفَّر.

(٥) دوال الاختزال

حتى الآن، ركَّزنا على خوارزميات التشفير التي يمكن استخدامها لتوفير السرية. تحظى هذه الخوارزميات بخاصية أساسية تتمثل في قابليتها لإجراء عمليات عكسية؛ وهو ما يعني أنه في حال معرفة المفتاح المناسب، يصبح من الممكن إعادة بناء رسالة النص الأصلي عبر النص المشفَّر. ومع ذلك يوجد حالات عديدة يجري فيها استخدام التشفير، لكن دون الحاجة إلى توفر القدرة على استنباط محتوى «الرسالة» الأصلية من صيغتها المشفرة. في حقيقة الأمر، ربما يوجد شرط يتطلب عدم إمكانية إجراء ذلك. نضرب مثالًا على ذلك، وهو حماية كلمات المرور في أحد أنظمة الكمبيوتر. يتلقى المستخدمون تعليمات بالحفاظ على سرية كلمات مرورهم؛ ومن ثَمَّ يصبح من المنطق بمكان افتراض أن النظام أيضًا يحاول ضمان هذه السرية. من هنا، متى ظهرت كلمات المرور في النظام، خاصةً في قاعدة البيانات المستخدمة في عملية التحقق، يجب تأمينها. ومع ذلك يتمثل الاشتراط هنا عادةً في القدرة على التحقق من صحة كلمة مرور جرى تسجيلها؛ ومن ثَمَّ ربما لا توجد حاجة إلى توفر القدرة على استنباط كلمة المرور من القيمة المخزَّنة.

هناك أيضًا العديد من الأمثلة في التشفير يجري فيها ضغط الرسائل الكبيرة إلى سلسلة قصيرة من الأرقام الثنائية (أقصر بكثير من طول الرسالة الأصلية). عندما يحدث ذلك، سيكون من الحتمي أن تُفضي أكثر من رسالة واحدة إلى نفس سلسلة الأرقام الثنائية الأقصر، وهذا تلقائيًّا يشير إلى أن عملية الضغط غير قابلة للعكس. يطلق على هذه الدوال اسم «دوال الاختزال» التي قد تتضمن أو لا تتضمن استخدامَ مفتاح تشفير، وذلك حسب التشفير المستخدم.

تتمثل الفكرة الأساسية لدوال الاختزال في أن قيمة التشفير المحوَّر الناتجة تمثل صورة مختصرة للرسالة الأصلية. وللقيمة الناتجة عن اختصار الرسالة الأصلية أسماء عدة؛ مثل «البصمة الرقمية»، و«مختصر الرسالة»، وبالطبع «قيمة التشفير المحوَّر».

تتضمن عملية التشفير المحوَّر عددًا من التطبيقات؛ منها تحقيق تكامل البيانات واستخدامها كجزء من عملية التوقيع الرقمي.

بوجه عام، تقبل دوال الاختزال مُدخَلات بأي طول وتُنتِج مُخرَجات ثابتة الطول. إذا أنتج مُدخلان المخرج نفسه، نطلق على ذلك «صدام». مثلما أشرنا، يعتبر وجود صدام مسألة حتمية. من هنا، إذا أردنا تحديد رسالة ما تحديدًا دقيقًا من خلال بصمتها الرقمية، يجب انتقاء دالة الاختزال جيدًا لضمان استحالة اكتشاف حالات الصدام حتى في حال وجودها. يترتب على ذلك عدد من النتائج، تتمثل إحداها في ضرورة ارتفاع عدد قيم البصمات الرقمية الممكنة. لبيان السبب في ذلك، نذكر مثالًا بسيطًا للغاية. إذا كانت هناك ثمانية قيم محتملة فقط للبصمة الرقمية، فسيكون هناك احتمالٌ نسبته ١٢٫٥٪ في أن يكون لرسالتين اعتباطيتين نفسُ القيمة. بالإضافة إلى ذلك، يكون من المضمون اشتمال أي مجموعة تتألف من تسع رسائل أو أكثر على حالة صدام واحدة على الأقل.

(٦) أنظمة المفاتيح المعلنة

تناولنا حتى الآن الخوارزميات المتناظرة التي يشترك فيها الطرفان المرسل والمستقبل في معرفة المفتاح السري. ينطوي ذلك بطبيعة الحال على توفر الثقة بين الطرفين. قبل أواخر السبعينيات من القرن العشرين، كانت تلك هي فقط الخوارزميات المتوفرة.

تتمثل الفكرة الأساسية لنظام التشفير ذي المفتاح المعلن في أن كل طرف له يحظى «بمفتاح معلن» و«مفتاح سري» مناظر له. يجري انتقاء هذه المفاتيح بحيث يصير من المستحيل استنباط المفتاح السري من المفتاح المعلن. ويحتاج كلُّ مَن يرغب في استخدام هذا النظام لإرسال رسالة سرية إلى شخص آخر إلى الحصول على المفتاح المعلن لذلك الشخص واستخدامه في تشفير البيانات. ومن الضرورة بمكان، بطبيعة الحال، شعور طرفِي المراسلة بالثقة في استخدام المفتاح المعلن الصحيح؛ لأنه في حال عدم تحقق ذلك، سيكون مالك المفتاح السري المناظر للمفتاح المعلن المستخدم، مقارنة بالطرف المستقبل، هو فقط من يستطيع فهم الرسالة. من هنا، على الرغم من عدم وجود حاجة إلى توزيع المفاتيح سرًّا، تحتاج جميع المفاتيح المعلنة إلى الحماية؛ وهو ما يعني ضرورة ضمان صحتها. من الجدير بالملاحظة أيضًا أنه في حال استخدام نظام المفاتيح المعلنة لتوفير السرية، بما أن مفتاح التشفير المعلن معروف على نطاق واسع كما يمكن لأي شخص استخدامه، لا يوفر النص المشفر أي طريقة يمكن من خلالها التحقق من هوية الطرف المرسل.

بالنسبة إلى نظام المفاتيح المعلنة، يعتبر كلٌّ مِن الخوارزمية ومفتاح التشفير معروفين (معلنين). وهكذا، يواجه الطرف المعترض مهمة محاولة استنتاج الرسالة من النص المشفَّر الذي جرى الحصول عليه من خلال أسلوب يعرفه معرفة تامة. بديهيًّا، يجب انتقاء عملية التشفير بعناية بالغة لضمان صعوبة مهمة الطرف المعترض. في المقابل، يجب عدم نسيان أن المتلقي الأصلي للرسالة يجب أن يمتلك القدرة على فك شفرة الرسالة بسهولة؛ لذا، يجب انتقاء عملية التشفير بحيث تيسِّر معرفة مفتاح فك التشفير عملية تحديد الرسالة من النص المشفَّر.

هذا مفهوم يصعب استيعابه. ثمة سؤال يُطرح كثيرًا وهو: «إذا كان الجميع يعرفون ما قمتَ به لتحديد النص المشفَّر، فلماذا إذن لا يفكون شفرة الرسالة؟» يساعد المثال غير الرياضي التالي عادةً في تقديم الإجابة.

هب أنك في غرفة مغلقة لا يوجد بها هاتف وقُدمت إليك نسخة ورقية من دليل الهاتف في لندن؛ إذا أعطاك أحد اسمًا وعنوانًا وسألك عن رقم هاتف صاحبهما، فستكون هذه مهمة سهلة. في المقابل، هب أن أحدهم أعطاك رقم هاتف عشوائيًّا وسألك عن اسم وعنوان صاحبه؛ تأكيدًا، هذه مهمة شاقة للغاية. لا يرجع السبب إلى عدم معرفتك بما يجب القيام به. فمن الناحية النظرية، قد تبدأ من الصفحة الأولى ثم تقرأ جميع الأرقام حتى تجد الرقم الصحيح. تكمن الصعوبة هنا في حجم المجهود المبذول؛ لذا، إذا نظرنا إلى «الاسم والعنوان» باعتبارهما الرسالة، وإلى «رقم الهاتف» باعتباره النص المشفَّر، وإلى «إيجاد رقم كذا» باعتباره عملية التشفير، فسنكون قد حققنا الهدف في حالة دليل الهاتف في لندن. من الأهمية بمكان الإشارة إلى أنه في حال تطبيق العملية نفسها على أدلة هاتف أصغر حجمًا، سيتمكن الطرف المعترض من إجراء عملية عكسية. بالإضافة إلى ذلك، لا يمكن التحديد على وجه الدقة عدد الأشخاص المطلوب قبل أن نشعر بأن لدينا أسبابًا قوية للادعاء بتحقيق الهدف. يتضمن دليل الهاتف في لندن أكثر من 750 ألف اسم، ونستطيع أن نقول ونحن مطمَئِنِّين إن 750 ألفًا يعتبر رقمًا ضخمًا في هذا السياق. بالنسبة إلى إحدى منشآت العمل التي لا تزيد فيها الأرقام الداخلية عن 100 رقم، يعتبر إجراء عملية عكسية لاستنباط عدد صحيح من بين قائمة الأرقام عملية سهلة على الأرجح. لكن ماذا عن دليل يشتمل على 5000 رقم؟

يوجد، بطبيعة الحال، مؤسسات معينة مثل خدمات الطوارئ التي تستطيع تحديد هوية مالكي أي أرقام هاتفية؛ إذ تمتلك هذه المؤسسات دليلًا مرتبًا ترتيبًا رقميًّا. نعيد

فنؤكد مرة أخرى، لا يوجد ما يمنع من بناء أي شخص نسخته الخاصة بترتيب رقمي. ضخامة المهمة هي التي تضمن عدم نجاحه في مساعيه وفق الظروف التي حددناها. في المقابل، تصبح المهمة أسهل كثيرًا في حال امتلاك أحدهم نسخة إلكترونية من الدليل.

معظم خوارزميات المفاتيح المعلنة العملية عبارة عن شفرات كُتل تتعامل مع الرسالة باعتبارها سلسلة من الأعداد الصحيحة الكبيرة، وتعتمد على صعوبة حل مسألة رياضية معينة لضمان تحقيق الأمن. ابتكر أكثر هذه الأنظمة شهرةً رون ريفست، وآدي شامير، ولين أدلمان في عام ١٩٧٨، وهو النظام المعرف اختصارًا باسم آر إس إيه. في هذا النظام، المسألةُ الرياضية المصاحبة للنظام هي عملية تحليل الأعداد إلى عواملها الأولية؛ حيث يوجد مفتاح معلن معروف N، وهو ناتج ضرب عددين أوليين قيمتاهما سريتان. هذان العددان في غاية الأهمية؛ حيث إن أي شخص يعرف قيمتيهما يستطيع حساب المفتاح السري من خلال المفتاح المعلن. لذا، يجب أن يكون العدد N، الذي يحدد طول كتلة الرسالة، كبيرًا بما يكفي بحيث لا يستطيع أي طرف معترض استنباط العددين الأوليين؛ بمعنى أنه لا يستطيع تحليل العدد N إلى عوامله الأولية. بداهةً، إذا كان العدد N صغيرًا، فسيستطيع أي شخص تحديد العددين الأوليين. كمثال بسيط على ذلك، افترض أنَّ $N = 15$؛ ومن ثَمَّ فالعددان الأوليَّان هما 3 و5. لكن يُعتقد أن اكتشاف العددين الأوليين مسألة غير ممكنة في حال كان العدد N كبيرًا بما يكفي. نناقش صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية في الفصل السابع. حاليًّا، نكتفي بالإشارة إلى أن العدد N يحدِّد طول كلٍّ مِن الكتلة والمفتاح.

يعني ذلك أن أطوال المفاتيح والكتل هي على الأرجح أكبر بكثير مما في حالة الشفرات المتناظرة. ففي حالة الشفرات المتناظرة، تعتبر الأطوال النموذجية للكتل هي 64 أو 128 رقمًا ثنائيًّا، فيما تبلغ في حالة نظام آر إس إيه 640 رقمًا ثنائيًّا على الأقل، كما لا تعتبر الكتل التي يبلغ طولها 1024 أو 2048 شائعة. من النتائج المترتبة أيضًا على استخدام نظام آر إس إيه أن عمليات التشفير وفك التشفير تتضمن إجراء العديد من الحسابات باستخدام أعداد كبيرة؛ وهو ما يعني بطء أنظمة الشفرات هذه مقارنةً بمعظم الخوارزميات المتناظرة. بناءً عليه، غالبًا ما لا تُستخدم هذه الأنظمة في تشفير كميات هائلة من البيانات، وإنما تستخدم على الأرجح في التوقيعات الرقمية أو كمفاتيح تشفير لمفاتيح أخرى لتوزيع أو تخزين مفاتيح الخوارزميات المتناظرة.

أما خوارزمية المفتاح المعلن الأخرى المستخدمة على نطاق واسع فهي «الجَمَل» (نسبة إلى مبتكرها طاهر الجمل) التي تشكِّل أساس «معيار التوقيع الرقمي» الأمريكي

«دي إس إس». بالنسبة إلى خوارزمية الجمل، تساوي أطوال المفاتيح أطوال نظيراتها تقريبًا في خوارزمية آر إس أيه، لكن الأمن فيها يعتمد على صعوبة حل مسألة رياضية مختلفة تُعرف باسم مسألة اللوغاريتم المتقطِّع. لكن نظام الجمل يمتلك خواص محددة لا تجعله يصلح في إجراء عمليات التشفير.

جرى تطوير المبادئ والأساليب القياسية لنظام تشفير المفاتيح المعلن في أوائل السبعينيات من القرن العشرين بواسطة جيمس إليس، وكليفورد كوكس، ومالكوم وليامسون في مجموعة أمن الاتصالات-الإلكترونيات التابعة لحكومة المملكة المتحدة. ومع ذلك كان هذا الجهد مدرجًا كمعلومات سرية غير مصرح بالاطلاع عليها لأكثر من عقدين، ولم تُعلَن هذه المعلومات إلا بعد ظهور أبحاث تشفير المفاتيح المعلنة الأولى بوقت طويل، بعدها تطورت أساليب التشفير غير المتناظر تطورًا كبيرًا.

الفصل السادس

الأمن العملي

(١) مقدمة

يُستخدم مصطلح «التشفير القوي» على نطاق واسع، لكنه يمكن أن يشير، دون عجب، إلى معانٍ مختلفة حسب كل شخص. عادةً يُفهم المصطلح بمعنى «عملية تشفير غير قابلة للكسر»، على الرغم من أن هذا التعريف في ذاته يعتبر تعريفًا أقل موضوعية مما قد يكون متوقعًا.

لعدة سنوات ساد الاعتقاد بأن نظام دفتر المرة الواحدة هو نظام التشفير الوحيد غير القابل للكسر. أثبت كلود شانون ذلك في بحثين مهمين في عامَيْ ١٩٤٨ و١٩٤٩. يعتبر هذان البحثان الأساس لنظرية الاتصالات الحديثة، بما في ذلك التشفير. في الواقع، لا يمكن التأكيد بما يكفي على أهمية إسهام شانون.

رأينا كيف أن استخدام دفتر المرة الواحدة لا يمكن تطبيقه عمليًّا في معظم الحالات. من هنا، تستخدم معظم الأنظمة العملية خوارزميات يمكن كسرها من الناحية النظرية. لكن هذا لا يعني بالضرورة أن هذه الخوارزميات غير آمنة. على سبيل المثال، إذا كانت جميع عمليات الاعتراض النظرية للخوارزميات صعبة جدًّا لدرجةِ تعذُّر تنفيذها، فربما يجد المستخدمون تبريرًا في النظر إلى خوارزميتهم على أنها غير قابلة للكسر. حتى إن لم يكن الأمر كذلك، ففي بعض التطبيقات تتخطى الموارد اللازمة لحل الخوارزمية قيمة الفائدة المحتملة كثيرًا بالنسبة إلى أي طرف معترض. في مثل هذه الحالة، سيُنظر إلى الخوارزمية باعتبارها «آمنة بما يكفي». هب — على سبيل المثال — أن أحد الأشخاص ينتوي استخدام التشفير لتحقيق السرية لبعض البيانات؛ يجب على هذا الشخص أولًا أن يجري عملية تقييم للبيانات التي تجري حمايتها، وهي عملية ربما لا تكون بسيطة؛ إذ

قد لا تكون قيمة البيانات نقدية بل شخصية محضة. من الأمثلة الواضحة على البيانات التي قد يستحيل وضع قيمة كمية لها، السجلاتُ الطبية والتفاصيل الشخصية الأخرى. يجب على هذا الشخص أيضًا إجراء نوع من التقييم حول هوية مَن يريد الاطلاع على بياناته، ولماذا. تتمثل العوامل الأخرى المهمة في التأثير على عملية حماية البيانات في الفترة التي يلزم الحفاظ على سرية البيانات خلالها، فضلًا عن تكلفة الخوارزمية وتوفرها وسهولة استخدامها.

عند إدماج التشفير في أحد الحلول الأمنية، يوجد أسلوبان قابلان للتعارض في اختيار خوارزمية التشفير:

- استخدام أقل مستويات الأمن التي تكفل تحقيق الحماية المناسبة.
- استخدام أقصى مستويات الأمن التي تسمح بها اعتبارات التنفيذ.

بداهةً، من الأهمية بمكان بالنسبة إلى المنفذين توفُّر معرفة جيدة لديهم بمستوى الأمن الذي توفره الخوارزمية، وهو ما نتناوله في الأجزاء الأخيرة من هذا الفصل. تركِّز المناقشة في الأساس على عمليات البحث الشاملة عن المفتاح في أنظمة الخوارزميات المتناظرة، وعلى عمليات الاعتراض التي تستهدف العمليات الرياضية الأساسية في أنظمة المفتاح المعلن. بطبيعة الحال، مثلما أكدنا سابقًا، فإن زمن عملية البحث الشاملة عن المفتاح المعلن يعطي حدًّا علويًّا لقوة الخوارزمية. توجد طرق أخرى للاعتراض أكثر سهولة. ومع ذلك نعتقد أن تصميم الخوارزميات متطور بما يكفي كي تكون هناك خوارزميات تشفير متعددة جيدة التصميم، بمعنى أن عملية البحث الشاملة عن المفتاح تمثِّل أسهل صور الاعتراض المعروفة. بالإضافة إلى ذلك، يكون تنفيذ هذه الخوارزميات على الأرجح سريعًا جدًّا.

في الماضي، غالبًا ما كانت اعتبارات التنفيذ تجبر المستخدمين على تبنِّي سياسة استخدام أقل مستويات الأمن الممكنة. وسرعان ما سايرت التكنولوجيا المتقدمة سياسات التنفيذ؛ وهو ما أدى إلى نتائج كارثية في كثير من الأحيان.

(٢) الأمن الواقعي

بيَّن شانون أن نظام دفتر المرة الواحدة يعتبر نظام الشفرة الوحيد الآمن تمامًا. وهكذا، نعرف على الأقل من الناحية النظرية أن معظم الأنظمة العملية يمكن كسرها. لكن هذا

لا يشير إلى أن معظم الأنظمة العملية غير ذات جدوى. قد يكون أحد أنظمة التشفير (القابلة للكسر نظريًّا) مناسبًا لأحد التطبيقات، إذا كان المستخدمون يشعرون بالثقة في استبعاد وقوع عملية اعتراض ناجحة قبل انقضاء فترة التغطية لهذا التطبيق.

تعتبر عملية البحث الشاملة عن المفتاح إحدى الصور الرئيسية للاعتراض التي ناقشناها سابقًا. والوقت التقديري اللازم لإجراء بحث شامل عن المفتاح، والذي يكون أطول بكثير من زمن التغطية، هو أحد «العقبات» الواضحة الواجب تخطيها في أنظمة التشفير قبل اعتبارها أنظمة مناسبة للاستخدام في تطبيقات محددة. بطبيعة الحال، رأينا كيف أنَّ توفر عدد كبير من المفاتيح لا يضمن توفر نظام آمن؛ وبناءً عليه، يعتبر اجتياز هذا الشرط أول اختبار بين اختبارات عديدة يجب إجراؤها قبل اعتبار أحد أنظمة التشفير نظامًا مقبولًا. ومع ذلك فإن الفشل في اجتياز هذا الاختبار علامة واضحة على عدم إمكانية استخدام الخوارزمية. من هنا، يتمثل «اختبارنا» الأول في أي نظام تشفير في محاولة معرفة أن الوقت اللازم لإجراء عملية بحث شاملة عن المفتاح يكون طويلًا بما يكفي، أو بطريقة أخرى مكافئة، أن عدد المفاتيح كبير بما يكفي.

لتنفيذ ذلك، يحتاج المصمم إلى وضع عدد من الافتراضات حول موارد الطرف المعترض وقدراته. تتمثل المهمة الأولى للمصمم في محاولة وضع تقدير للوقت اللازم الذي يستغرقه الطرف المعترض في تجربة مفتاح واحد. بداهةً، يعتمد هذا الوقت على ما إذا كان الطرف المعترض يستخدم أجهزة أو برامج. ففي حال الاعتراض باستخدام أجهزة، قد يستخدم الطرف المعترض جهازًا مصممًا لغرض معين. وعلى الأرجح سيؤدي سوء تقدير هذا الوقت نقصانًا إلى عدم تحقيق الأمن، فيما سيؤدي سوء تقدير الوقت زيادة إلى جعل عملية توفير الأمن عبئًا أكبر مما ينبغي.

ربما يتوصل أحد الأطراف المعترضة المحظوظة، عند إجرائه عملية بحث شاملة عن المفتاح إلى المفتاح من أول عملية تخمين. تتمثل إحدى نتائج توفر عدد كبير من المفاتيح في جعل احتمال حدوث ذلك ضئيلًا للغاية. على النقيض، ربما لا يكتشف الطرف المعترض غير المحظوظ المفتاح إلا عند المحاولة الأخيرة. عمليًّا، يُستبعد إجراء الطرف المعترض عملية بحث كاملة عن المفتاح قبل العثور عليه. ويقترب الوقت المتوقع لاكتشاف المفتاح من خلال عملية بحث اقترابًا كبيرًا من نصف الوقت اللازم لإجراء عملية بحث شاملة وكاملة.

ربما تجدر الإشارة في هذه المرحلة — على سبيل المثال — إلى أنه في حال توفر بيانات كافية لدى الطرف المعترض، ربما سيشعر بالثقة في أن مفتاحًا واحدًا قد يحوِّل

النص الأصلي كاملًا إلى النص المشفر الصحيح. لكنه في العديد من الحالات، قد لا يسفر إجراء عملية بحث شاملة عن تحديد مفتاح واحد صحيح، بل يؤدي إلى تقليص عدد المفاتيح الصحيحة المحتملة، فيما يجب إجراء المزيد من البحث في ظل توفر المزيد من البيانات.

بمجرد تحديد عدد المفاتيح، فإن الوقت اللازم لإجراء عملية بحث شاملة عن المفتاح يعتبر حدًّا أقصى لمستوى الأمن المطلوب. في العديد من الحالات، يتمثل هدف المصمم الرئيسي في محاولة ضمان كون الوقت المتوقَّع لنجاح طرف معترض آخر في التوصل إلى المفتاح الصحيح أطول من هذا الحد الأقصى، وهي ما لا تعد مهمة سهلة. استخدمنا كلمات تشير إلى أن الوقت هو المقياس المناسب لتقييم احتمالية نجاح عملية الاعتراض. ومع ذلك يعتمد الوقت اللازم لإجراء أي عملية حسابية على عدد من المتغيرات؛ منها — على سبيل المثال — القدرة المتاحة لمعالجة البيانات، والقدرة الفنية/الرياضية لدى الأطراف المعترضة. ترتبط القدرة المتاحة لمعالجة البيانات على الموارد المالية المتوفرة لدى الطرف المعترض، وهي الموارد، التي تعتمد بدورها على الفائدة المتوقعة من تنفيذ عملية اعتراض ناجحة. بالإضافة إلى ذلك، في بعض الحالات، تعتبر بعض الأمور الأخرى، مثل توفر ذاكرة كمبيوتر ضخمة لدى الطرف المعترض، أمورًا مهمة. وبأخذ كل ذلك في الاعتبار، تعتبر، مع ذلك، هذه الإجراءاتُ المعقدةُ الطريقةَ المعتادة لتحديد ما إذا كان أحد الأنظمة آمنًا بما يكفي لاستخدامه في أحد التطبيقات.

(٣) العمليات الشاملة العملية للبحث عن المفتاح

على الرغم من عدم رغبتنا في ذكر أي عمليات حسابية معقدة، ربما تجدر الإشارة إلى بعض الحقائق بحيث «نستشعر» عدد المفاتيح المطلوبة في بعض الحالات. بداهةً، ربما يرغب أي شخص يسعى إلى تصميم نظام لتطبيق تجاري في أن يكون هذا النظام آمنًا (على الأقل) لبضع سنوات؛ ومن ثَمَّ يجب أخذ أثر تطور التكنولوجيا في الاعتبار. يجري ذلك من خلال تطبيق قاعدة عملية تسمى «قانون مور» الذي ينص على أن القدرة الحسابية المتاحة في ضوء تكلفة محددة تتضاعف كل ١٨ شهرًا.

حتى نستشعر طول المفاتيح في بعض الأحيان، تجدر الإشارة إلى أن السنة تشتمل على 31536000 ثانية، وهو رقم يقع بين قيمتَيْ 2^{24} و2^{25}. إذا حاول أحد الأشخاص تجربة مفتاح واحد في الثانية، فسيستغرق الأمر أكثر من سنة للانتهاء من إجراء عملية

بحث عن المفتاح ضمن 2^{25} مفتاح. في المقابل، إذا توفر لدى هذا الشخص كمبيوتر يستطيع تجربة مليون مفتاح كل ثانية، فسيكون الوقت اللازم للبحث في 2^{25} مفتاح أقل بكثير من دقيقة واحدة. هذا فارق عظيم، وعلى الرغم من بساطته، فإنه يشير إلى الأثر الذي تَرَتَّب على ظهور الكمبيوتر في عدد المفاتيح اللازمة لتصميم أنظمة آمنة. عند مناقشة خوارزميات التشفير، يشير بعض المؤلفين إلى طول المفتاح فيما يشير آخرون إلى عدد المفاتيح. تجدر الإشارة إلى أنه توجد 2^S سلسلة من الأرقام الثنائية (بتات) بطول S؛ وهو ما يعني أنه إذا كان كل شكل محتمل من الأرقام الثنائية يمثل مفتاحًا، فإن القول بأن نظام التشفير له مفاتيح عبارة عن S من الأرقام الثنائية يكافئ القول بأن النظام له 2^S مفتاح. تجدر الإشارة أيضًا إلى أنه في حال كان كل نمط متكرر محتمل من الأعداد الثنائية يمثل مفتاحًا، فإن إضافة رقم ثنائي واحد زائد إلى طول المفتاح مماثلة لمضاعفة عدد المفاتيح.

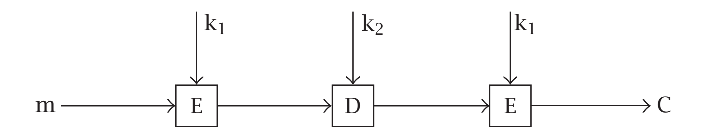
يعتبر أكثرَ نظام شفرات الكتل شهرةً نظامُ «معيار تشفير البيانات». نُشر هذا المعيار في عام ١٩٧٦ وجرى استخدامه على نطاق واسع في القطاع المالي. يتضمن نظام معيار تشفير البيانات 2^{56} مفتاح، ومنذ اللحظة الأولى لإصداره، دارت مناقشات حول مدى قوته. في عام ١٩٩٨، صَممتْ وأَنشأتْ مؤسسةٌ تسمى مؤسسة الحدود الإلكترونية جهازًا خاصًّا لإجراء عمليات البحث الشاملة عن المفاتيح بنظام معيار تشفير البيانات.

بلغت التكلفة الإجمالية 250 ألف دولار أمريكي، وكان من المتوقع إيجاد مفتاح في غضون خمسة أيام. على الرغم من أن مؤسسة الحدود الإلكترونية لا تدعي أنها أجرت التطوير الأمثل لتصميمها، ظل الجهاز الأصلي بمنزلة دليل يُهتدى به إلى الآن. ففي ظل توفر 250 ألف دولار أمريكي، نستطيع القول بصورة تقريبية إنه من الممكن بناء ماكينة تستطيع إجراء عملية بحث بين 2^{56} مفتاح في غضون أسبوع. يمكن التوسع الآن في هذا عن طريق زيادة تكلفة أو زيادة عدد المفاتيح، وبعد تضمين عاملٍ ما في التصميم مثل قانون مور، نستطيع الحصول على تقديرات أولية بالوقت اللازم لإجراء عملية بحث خلال عدد محدد من المفاتيح، في ضوء ميزانية محددة، في أي وقت في المستقبل القريب.

بالإضافة إلى الأجهزة التي جرى بناؤها لغرض محدد كانت توجد ولا تزال أعداد من الجهود في مجال عمليات البحث الشاملة عن المفاتيح المعلنة، والتي عادة ما تَستخدم القدرة الحسابية المجمعة من خلال عمليات بحث مفتوحة عن المفاتيح عبر الإنترنت. لعل من أهم هذه الجهود على الإطلاق، جهدًا كُلِّل بالنجاح في يناير ١٩٩٩. اعتمد أسلوب

البحث في ذلك المسعى على مزيج من جهاز مؤسسة الحدود الإلكترونية والتعاون عبر الإنترنت فيما تضمن استخدام أكثر من 100 ألف كمبيوتر، ولم يستغرق الأمر إلا أقل من يوم واحد فقط لاكتشاف مفتاح نظام معيار تشفير البيانات بطول 56 رقمًا ثنائيًّا.

ركَّزنا على عمليات البحث من خلال نظام معيار تشفير البيانات؛ نظرًا لأهمية هذه الخوارزمية. عندما جرى تصميم هذه الخوارزمية في منتصف سبعينيات القرن العشرين، كانت تُعد خوارزمية قوية. حاليًّا، بعد مرور 25 عامًا فقط، يجري العثور على مفاتيح نظام معيار تشفير البيانات في أقل من يوم. جدير بالملاحظة أن نجاح عمليات البحث الأخيرة عن مفاتيح معيار تشفير البيانات لم تُثِرْ دهشة المستخدمين الحاليين للنظام أو مصمميه، الذي أوصوا (في عام ١٩٧٦) باستخدامه لمدة 15 عامًا. ينفذ معظم المستخدمين الحاليين ما يطلق عليه اسم معيار تشفير البيانات الثلاثي. في هذه الحالة، يتألف المفتاح من مفتاحين أو ثلاثة بنظام معيار تشفير البيانات (112 أو 168 رقمًا ثنائيًّا). يبين الشكل التالي مفتاح معيار تشفير البيانات الثلاثي المؤلَّف من المفتاحين k1 وk2؛ حيث يمثِّل كلٌّ من E وD التشفير وفك التشفير على الترتيب.



معيار تشفير البيانات الثلاثي ثنائي المفاتيح.

حتى ندرك مدى الأثر الكبير الذي يتولد عن إضافة ثمانية أرقام ثنائية زائدة إلى المفتاح، نشير إلى أن أول عملية بحث أُجريت عبر الإنترنت عن مفتاح طوله 64 رقمًا ثنائيًّا لخوارزمية أُطلق عليها RC5 بدأت في عام ١٩٩٨. بعد أكثر من 1250 يومًا جرى تجربة ٤٤٪ من إجمالي عدد المفاتيح المحتملة ولم يكن قد جرى اكتشاف المفتاح الصحيح بعد.

في عام ٢٠٠١، نَشر المعهد القومي للمعايير والتكنولوجيا خوارزمية تشفير جديدة «يمكن استخدامها لحماية البيانات الإلكترونية». أُطلق على هذا الخوارزمية اسم «معيار التشفير المتقدم»، وجرى انتقاؤها من بين عدد من الخوارزميات التي جرى تقديمها استجابة إلى طلب من المعهد. كانت الاشتراطات المطلوبة تتمثل في وضع شفرة كتل

متناظرة، يمكن من خلالها استخدام المفاتيح 128، و192، و256 رقمًا ثنائيًّا (بتًا) لتشفير وفك تشفير البيانات الموجودة في مجموعات من 128 رقمًا ثنائيًّا. يطلق على الخوارزمية المُنتقاة اسم ريندال، صممها بلجيكيَّان؛ جون دامون وفنسنت ريمون. وحيث إن نظام معيار التشفير المتقدم يتضمن مفتاحًا يبلغ الحد الأدنى لطوله 128 رقمًا ثنائيًّا، يبدو نظام التشفير هذا محصنًا ضد عمليات البحث الشاملة عن المفاتيح باستخدام التكنولوجيا الحالية.

ذكرنا آنفًا أن قانون مور يقدم تقديرًا تقريبيًّا بالتحسينات في التكنولوجيا الحالية خلال السنوات القليلة المقبلة. ولا يركِّز قانون مور على التكنولوجيات الجديدة الشديدة التطور التي قد يكون لها أثر هائل، منها تكنولوجيا الحوسبة الكمية. تنفذ الحوسبة الكمية عمليات حسابية باستخدام حالات كمية تسمح بإجراء نوع من العمليات الحسابية المتوازية. حاليًّا، جرى بناء أجهزة كمبيوتر كمية صغيرة الحجم للغاية؛ لذا هي في الأساس مفهوم نظري. ومع ذلك إذا صارت أجهزة الكمبيوتر الكمية واقعًا في يوم من الأيام، سيتغير الوضع تمامًا. تُنفَق أموال طائلة حاليًّا حول العالم على دعم بحوث تطوير الحوسبة الكمية. إذا أمكن بناء أجهزة كمبيوتر كمية معقدة، فستجعل عملية البحث الشاملة عن المفاتيح أسرع كثيرًا. كمثال بسيط على ذلك، سيُضاعِف الكمبيوتر الكمي من طول المفتاح الذي يجري البحث عنه خلال وقت محدد. على سبيل المثال، يمكن القول على نحو تقريبي بأنه ستُساوي سرعة عملية البحث بين 2^{128} مفتاح من خلال كمبيوتر كمي سرعة البحث بين 2^{64} مفتاح الآن.

لا يزال الباحثون يتوخَّوْن الحيطة فيما يتعلق باحتمالات بناء كمبيوتر كمي. في المقابل، لا يزال البعض متفائلًا ويجب عدم استبعاد إمكانية تحقيق ذلك.

(٤) عمليات اعتراض أنظمة المفاتيح المعلنة

في حين يزيد طول مفاتيح الخوارزميات غير المتناظرة عن الخوارزميات المتناظرة، لا يعني ذلك أن الخوارزميات غير المتناظرة أكثر قوة بالضرورة. ولا تعتبر عمليات البحث الشاملة عن المفتاح أسلوبًا مناسبًا لاعتراض الخوارزميات غير المتناظرة. فبالنسبة إلى الخوارزمية غير المتناظرة، فمن السهولة بمكان محاولة حل المسألة الرياضية المرتبطة بالخوارزمية. على سبيل المثال، بالنسبة إلى نظام تشفير آر إس إيه، تعتبر عملية تحليل

المقياس الحسابي N إلى عوامله الأولية أسهل من إجراء عملية بحث شاملة عن المفتاح بين جميع مفاتيح فك التشفير المحتملة.

لبيان أثر التطورات الحديثة في العلوم الرياضية على نظام التشفير ذي المفتاح المعلن، نركِّز على نظام آر إس إيه وعملية تحليل العوامل. تنطبق ملاحظات مشابهة على أنظمة مفاتيح معلنة أخرى تعتمد على مسائل رياضية مختلفة.

تقدمت عملية تحليل العدد لعوامله الأولية تقدمًا هائلًا في الثلاثين سنة الأخيرة، وهو ما يرجع إلى تطورات على المستويين التكنولوجي والنظري. ففي عام ١٩٧٠، جرى تحليل عدد مؤلف من 39 رقمًا ($2^{128} + 1$) إلى عددين أوَّليَّيْن. في ذلك الوقت، كان ذلك إنجازًا عظيمًا. عند نشر نظام آر إس إيه للمرة الأولى عام ١٩٧٨، قَدَّمَ البحث رقمًا مؤلفًا من 129 رقمًا لتحليله إلى عوامله كتحدٍّ لصعوبة التحليل وعرضت جائزة 100 دولار أمريكي. كان ذلك واحدًا من سلسلة من التحديات المماثلة. على أي حال، لم يُجرَ تحليل العدد إلى عوامله إلا في عام ١٩٩٤، وجرى استخدام شبكة واسعة من أجهزة الكمبيوتر حول العالم.

25195908475657893494027183240048398571429282126204
03202777713783604366202070759555626401852588078440
69182906412495150821892985591491761845028084891200
72844992687392807287776735971418347270261896375014
97182469116507761337985909570009733045974880842840
17974291006424586918171951187461215151726546322822
16869987549182422433637259085141865462043576798423
38718477444792073993423658482382428119816381501067
48104516603773060562016196762561338441436038339044
14952634432190114657544454178424020924616515723350
77870774981712577246796292638635637328991215483143
81678998850404453640235273819513786365643912120103
97122822120720357

بالإضافة إلى قانون مور، تُعتبر احتمالية تحقيق تقدُّم في أساليب إجراء عمليات تحليل العدد لعوامله الأولية مسألةً أخرى تؤخذ في الاعتبار عند تحديد طول مفتاح

جرى تصميمه وفق نظام آر إس إيه. لبيان ذلك، نشير إلى الأثر الهائل الذي تحقق من خلال الاكتشاف الرياضي، الذي يحمل اسم «تنقية حقل الأعداد العامة»، الذي نُشر في عام ١٩٩٣. كان هذا الاكتشاف يعني أن الموارد اللازمة التي كانت تَستخدم خوارزميات معروفة سابقًا لتحليل أعداد بطول محدد إلى عواملها صارت تستخدم لتحليل أعداد أكبر بكثير. على سبيل المثال، بينما كانت الموارد اللازمة تُستخدم في تحليل رقم يتألف من 150 رقمًا إلى عوامله، صارت الآن تُستخدم في تحليل رقم يقترب من 180 رقمًا إلى عوامله. تَجاوز هذا الاكتشاف الرياضي جميع التطورات المتوقعة في أداء الابتكارات التكنولوجية خلال عدة سنوات.

جرى تحليل عدد التحدي المؤلف من 155 رقمًا، آر إس إيه-512، إلى عوامله باستخدام هذا الأسلوب في عام ١٩٩٩. استغرقت عملية التحليل إلى عوامله أقل من ثمانية أشهر، وهنا أيضًا استُخدمت شبكة عالمية من أجهزة الكمبيوتر. يتمثَّل مدى التعقيد الرياضي لمسألة التحليل في أن المرحلة الأخيرة منها تتضمن حل أكثر من ستة ملايين معادلة آنيًّا. تلا ذلك تحدٍّ نُشر في «كتاب الشفرات»، تطلَّب تحليل عوامل مقياس حسابي مؤلَّف من 512 رقمًا ثنائيًّا. تعتبر عمليات تحليل عوامل الأعداد في غاية الأهمية؛ إذ إن المقياس الحسابي بهذا الطول (155 رقمًا أو 512 رقمًا ثنائيًّا) كانت تُستخدم عادةً في أنظمة التشفير ذات المفتاح المعلن منذ سنوات قليلة مضت.

تتراوح التوصيات الحالية حول طول المقياس الحسابي لنظام آر إس إيه بين قيمتَيْ 640 و2048 رقمًا ثنائيًّا، وهو ما يعتمد على مستوى الأمن المطلوب. يتضمن العدد المؤلَّف من 2048 رقمًا ثنائيًّا على 617 رقمًا عشريًّا. لبيان ضخامة هذا الرقم، نقدِّم الرقم الذي جرى تصميمه وفق نظام آر إس إيه بنفس هذا القدر من الطول. تنتظر الشهرةُ وجائزةٌ قدرها 200 ألف دولار أمريكي أوَّلَ فريق يستطيع تحليل هذا العدد إلى عوامله بنجاح.

عند مناقشة عمليات البحث الشاملة عن المفاتيح، ذَكرنا الأثر المحتمل للكمبيوتر الكمي. وعلى الرغم من أن الكمبيوتر الكمي سيؤدي إلى زيادة هائلة في طول المفاتيح المتناظرة، لا يوجد شك في أن مجتمع التشفير سيتكيَّف مع ذلك الوضع، وأن الاستخدام الآمن للخوارزميات المتناظرة سيتواصل. ربما لا ينطبق الأمر نفسه على أنظمة المفاتيح المعلنة؛ ففي حال هذه الأنظمة، ستمثِّل الحوسبة الكمية تهديدًا أكثر جدية. على سبيل المثال، ستصبح عملية تحليل الأعداد إلى عواملها أكثرَ سهولة. لحسن الحظ، حتى أكثر المتحمسين للحوسبة الكمية لا يتوقعون بناءَ كمبيوتر كمي ضخم قبل 20 عامًا على الأقل.

الفصل السابع

استخدامات التشفير

(١) مقدمة

حتى الآن، افترضنا استخدام خوارزميات التشفير لتوفير السرية، لكن توجد تطبيقات أخرى كثيرة له. متى استخدمنا التشفير، فمن الأهمية بمكان التأكد من مساعدته لنا على تحقيق أهدافنا المرغوبة. نبين فيما يلي أحد الأمثلة على إساءةٍ محتملة لاستخدام التشفير.

في عام ١٩٨٣، أصدرتْ شركة إم جي إم فيلمًا اسمه «ألعاب الحرب». صار الفيلم أيقونة شعبية سلطت الضوء على مخاطر القرصنة. إحدى النبذات المختصرة عن الفيلم تَصِفُه بالقول: «يقع مصير البشرية في يد مراهق اخترق مصادفةً جهازَ الكمبيوتر التكتيكي لوزارة الدفاع.» يُظهر المشهدُ الافتتاحيُّ للفيلمِ المراهقَ وهو يحاول اختراق نظام الكمبيوتر في الجامعة وتغيير درجات صديقته. في ذلك الوقت، كانت كثير من الجامعات تخزِّن نتائج الاختبارات في قواعد بيانات يمكن الاطلاع عليها عن بعد. ولا عجب أن كثيرًا من الجامعات شعرت بالقلق من أن تتعرض نتائج الاختبارات فيها إلى مثل هذا النوع من التلاعب غير المصرح به كما ظهر في الفيلم، وأرادت توفير الحماية المناسبة لأنظمة الكمبيوتر بها.

تَمثَّل أحد الاقتراحات في تشفير درجات كل طالب. غير أن هذا لم يحقق الهدف المطلوب، ومن الأهمية بمكان، بل من المثير، معرفةُ سبب ذلك. من السهل معرفة ما تُحققه عملية تشفير الدرجات. تتمثل نتيجة عملية التشفير في أن أي شخص ينجح في اختراق قاعدة البيانات لن يستطيع الاطلاع على درجات أيٍّ مِن الطلاب. بدلًا من ذلك، سَيرى هؤلاء بياناتٍ لا معنى لها ترتبط بكل اسم. لسوء الحظ، لا يمنع ذلك بالضرورة القراصنة من إجراء عملية تغيير بناءة للدرجات. فإذا نجح القرصان في مسعاه، وتصادف معرفته بحصول طالب معين على درجات جيدة، فسيغيِّر فقط البيانات التي

لا معنى لها إلى جانب اسمه بحيث تصير مطابقة للبيانات إلى جانب اسم الطالب الآخر. بطبيعة الحال، إذا لم يعرف القرصان درجات الطالب الآخر تحديدًا، فإنه لن يعرف درجاته الجديدة الخاصة به هو. ومع ذلك يعرف القرصان الآن أنه حاصل على درجات نجاح. يعتبر هذا مثالًا واحدًا ضمن أمثلة عديدة على فشل استخدام التشفير في تحقيق أهداف المستخدم. فلا يعتبر التشفير حلًّا لجميع المشكلات. لاحظْ أيضًا، في هذا المثال تحديدًا، عدم حل شفرة الخوارزمية. في حقيقة الأمر، لم يَتم حتى إجراء عملية اعتراض لفك الشفرة. يتمثل كل ما جرى في أن المستخدم فشل في تحليل المسألة على وجه صحيح.

الاسم	الدرجات المشفرة
جيد	13AE57B8
سيئ	2AB4017E

←

الاسم	الدرجات المشفرة
جيد	13AE57B8
سيئ	13AE57B8

أو حتى

الاسم	الدرجات المشفرة
جيد	2AB4017E
سيئ	13AE57B8

هب الآن أن الجامعات شفَّرت قاعدة البيانات بالكامل، بدلًا من تشفير الدرجات فقط؛ هل كان ذلك سيحقق هدفَ منعِ القرصان من تغيير الدرجات؟ في هذه الحالة، يشير تشفير قاعدة البيانات كاملةً إلى أن الملف بأكمله لن يكون مفهومًا بالنسبة إلى القرصان. ولكن حتى في هذه الحالة، قد لا يكفي تحقيق الحماية ضد أي عمليات قرصنة لتغيير الدرجات. هب — على سبيل المثال — أن كل سطر في ملف قاعدة البيانات كان يمثل اسمَ ودرجاتِ كلِّ طالب؛ إذا كان ظهور أسماء الطلاب في قاعدة البيانات يجري وفق الترتيب الأبجدي لأسمائهم في الصف، فستظل تتوفر إمكانية وقوع عملية الاعتراض التي جَرَتْ مناقشتها في الفقرة السابقة.

قبل أن نتحول إلى التركيز على طريقة استخدام التشفير لحماية المعلومات المخزَّنة من التلاعب بها، نقف أولًا لنرى إذا كان من الأهمية بمكان أن يحاول أحد الأشخاص تغيير الدرجات في أي قاعدة بيانات. بطبيعة الحال، من المهم الإشارة إلى ضرورة منح

الطلاب الدرجات التي يستحقونها. وإذا لم تكن قاعدة البيانات هي السجل الوحيد المتوفر للدرجات، فلن يتحصل الطالب على أي فائدة جراء تغيير الدرجات في قاعدة البيانات. يتمثل الاشتراط الجوهري على الأرجح في ضرورة توفر آليةٍ ما لتحذير جميع المستخدمين المصرح لهم بأن الدرجات قد غُيِّرت. بناءً عليه، قد لا يكون منع عملية تغيير الدرجات أمرًا مهمًّا، شريطة توفُّر القدرة على اكتشاف أي تعديل في الدرجات. ربما يعني ذلك تنبيه المستخدمين المصرح لهم بعدم الاعتماد على قاعدة البيانات واللجوء إلى السجل الرئيسي. في كثير من الحالات، يكون مطلوبًا اكتشافُ التغييرات غير المصرح بها وليس منعُها.

يُستخدم التشفير عادة لضمان اكتشاف عمليات التغيير غير المصرح بها للوثائق. في الواقع، لم يَعُدْ تحقيق السرية، على الأقل بالنسبة إلى القطاع التجاري، هو أهمَّ تطبيقات عملية التشفير. فبالإضافة إلى استخدامه التقليدي في أغراض الخصوصية، يُستخدم التشفير حاليًّا لتوفير الآتي:

- «سلامة البيانات»: ضمان عدم تغيير البيانات عن طريق وسائل غير مصرح بها أو غير معروفة.
- «اعتماد الكيانات»: تحقيق هُويَّة كِيانٍ ما.
- «التحقق من مصدر البيانات»: تحقيق مصدر المعلومات.
- «عدم الإنكار»: الحيلولة دون إنكار محتوى المعلومات (عادةً من خلال المصدر) و/أو هوية المصدر.

بطبيعة الحال، يوجد عدد من الأساليب القياسية (غير التشفيرية) لحماية البيانات من التغيير الطارئ؛ مثل استخدام أسلوب تدقيق تكافؤ البيانات، أو أسلوب ترميز أكثر تطورًا لتصويب الأخطاء. إذا كان توفير الحماية ضد التغيير العمدي للبيانات مطلوبًا فإن هذه الأساليب قد لا تكون كافية؛ لأنها تعتمد على معلومات علنية. سيُجري كلُّ مَن يغير المعلومات عمدًا عمليةَ ترميز الرسالة المعدلة على نحو مناسب؛ بحيث لا يمكن اكتشاف عملية التغيير. بناءً عليه، لتحقيق الحماية ضد عملية التغيير العمدي للبيانات، يجب استخدام قيمة معينة لا يعرفها سوى الطرف المرسل و(ربما) الطرف المستقبل، كمفتاحٍ تشفيري مثلًا.

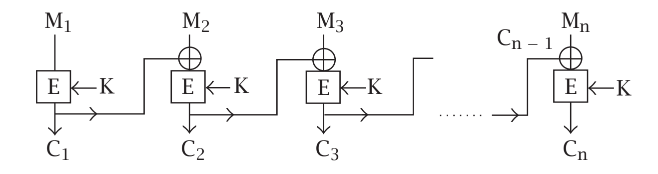
(٢) استخدام الخوارزميات المتناظرة لتحقيق السرية

وضعْنا أيديَنا على بعض المخاطر الأمنية المحتملة في حال استخدام نظام شفرات الكتل لتشفير البيانات وفق نمط كتاب الشفرات الإلكتروني. يتمثل أحد هذه المخاطر في إمكانية تلاعُب أحد الأشخاص ممن يعرفون كتل النص الأصلي والنص المشفر المتقابلين لبناء نص مشفَّر يستطيع من خلاله فك الشفرة إلى رسالة ذات معنًى. لن يستطيع الطرف المستقبِل اكتشاف التعديلات التي جرى إدخالها. رأينا قبلًا مثالًا بسيطًا على ذلك. لكن يجب أَن يجري التركيز هنا على كلمة «ذات معنًى». فإذا جرى استخدام نظام شفرة كتل وفق نمط كتاب الشفرات الإلكتروني، فسيكون من الممكن إعطاء خوارزمية فك التشفير كتلَ النص المشفر في أي ترتيب؛ ومن ثَمَّ ستتمكن من فك شفرة كل كتلة على حدة لإنتاج رسالة نهائية محتملة. ومع ذلك من غير المحتمل أن تمثِّل البيانات الناتجة عن فك الشفرة رسالة مترابطة منطقيًّا ومفهومة. وعلى الرغم من ضرورة عدم تجاهل إمكانية حدوث مثل هذا النوع من الاعتراضات، لا تزال فرص نجاحها ضئيلة.

تتمثل أكثر مساوئ استخدام نمط كتاب الشفرات الإلكتروني خطورةً في أن الطرف المعترض قد يتمكن من بناء قواميس تتألف من الكتلِ المعروفةِ للنص الأصلي ونص التشفير المتقابلةِ في ضوء استخدام مفتاح محدد، كما يصبح نمط كتاب الشفرات الإلكتروني معرضًا لعمليات اعتراض تعتمد على إجراء عمليات إحصائية للُّغة المستخدمة في النص الأصلي. والمثال «الكلاسيكي» لمثل هذا النوع من الاعتراضات هو مثال نظام شفرات الاستبدال البسيط الذي ذكرناه في الفصل الثالث.

يرجع سبب وجود أوجُه القصور هذه إلى أن الكتل يجري تشفيرها على نحوٍ مستقلٍّ بعضُها عن بعض. بناءً عليه، في ضوء وجود مفتاح محدد، ينشأ عن الكتل المتناظرة في النص الأصلي كتلٌ متناظرة في النص المشفر. تتمثل إحدى طرق التغلُّب على ذلك في جعْل كل كتلة في النص المشفر لا تعتمد فقط على الكتلة في النص الأصلي المقابلة لها، بل أيضًا على موضعها في النص الكامل. كان ذلك هو الأسلوبَ المتبع في نظام شفرة فيجنر. لا شك في أن هذه الأساليب تؤدي إلى «تسطيح» تأثير الإحصاءات اللغوية. لكن أحد الأساليب الشائعة والفعالة يتمثل في ضمان اعتماد الكتل في النص المشفر المقابلة للكتل في أي نص أصلي على محتويات الكتل في جميع النصوص الأصلية السابقة في الرسالة. يعتبر نمطُ تسلسل شفرات الكتل ونمطُ التغذية المرتدة للشفرات هما النمطَيْن الأكثر شيوعًا لتحقيق ذلك. نناقش نمط تسلسل شفرات الكتل.

هب أن لدينا رسالة تتألف من العدد n من الكتل، $M_1, M_2, \ldots, M_n$، ونرغب في تشفيرها باستخدام شفرات الكتل مع استخدام مفتاح K؛ في حال استخدام نمط تسلسل شفرات الكتل، يتضمن النص المشفَّر الناتج عدد n من الكتل، $C_1, C_2, \ldots, C_n$، لكن كل كتلة من كتل النص المشفَّر هذه تعتمد الآن على جميع الكتل السابقة للرسالة. تتمثل طريقة تنفيذ ذلك في الحصول على كل كتلة في النص المشفَّر، بخلاف الكتلة C_1، من خلال تشفير ناتج عملية إكس أو آر بين كتلة الرسالة المقابلة مع كتلة النص المشفر السابق له. على سبيل المثال، نجد أن C_2 هي نتاج تشفير $M_2 \oplus C_1$؛ لذا، إذا كتبنا EK لتمثيل عملية تشفير باستخدام المفتاح K، نحصل على $C_2 = EK(M_2 \oplus C_1)$. بداهةً، يجب التعامل مع الكتلة الأولى للرسالة على نحو مختلف. يتمثل أحد خيارات تحقيق ذلك في جعل C_1 تساوي $EK(M_1)$. ثمة خيار آخر شائع يتمثل في استخدام قيمة ابتدائية (IV) وجعل C_1 نتاج تشفير $M_1 \oplus IV$ (لاحظ في حال كانت جميع القيم في IV تساوي أصفارًا، ستتماثل نتيجة هذين الخيارين). وبما أن C_1 تعتمد على M_1، فيما تعتمد C_2 على M_2 وC_1، يبدو من الواضح اعتماد C_2 على كلٍّ مِن M_1 وM_2. بالمثل، بما أن $C_3 = EK(M_3 \oplus C_2)$، تعتمد C_3 على M_1 وM_2، وM_3. على وجه العموم، تعتمد كل كتلة في النص المشفر على الكتلة المقابلة لها في النص الأصلي وعلى جميع الكتل السابقة لها في النص الأصلي، وهو ما يترتب عليه ربْطُ جميعِ كتلِ النصِّ المشفَّرِ معًا في ترتيب محدد صحيح. لا تتخلص هذه الطريقة من الإحصاءات اللغوية في الرسالة فحسب، بل تَقْطع الطريق أيضًا أمام إمكانية التلاعب بالنص المشفر.



نمط تسلسل شفرات الكتل.

نبين الآن كيفية تطبيق نمط تسلسل شفرات الكتل من خلال مثال بسيط لشفرة كتل استخدمناه في الفصل الخامس، ومقارنةِ النصوص المشفَّرة عن طريق استخدام

الخوارزمية نفسها ومفتاح وفق نمط كتاب الشفرات الإلكتروني ونمط تسلسل شفرات الكتل. لسوء الحظ، يبدو المثالُ أكثرَ تعقيدًا مما هو عليه في حقيقة الأمر. نشجع القراء على المثابرة. ومع ذلك لا بأس من الانتقال مباشرةً إلى بداية القسم التالي.

في هذا المثال، النص الأصلي، المكتوب وفق نظام التمثيل السادس عشر، هو A23A9 والمفتاح K = B. تنفذ خوارزمية التشفير عملية إكس أو آر على كتلة النص الأصلي مع المفتاح، ويجري الحصول على كتلة النص المشفر من خلال تدوير الأرقام الثنائية لـ $M \oplus K$ موضع واحد إلى اليسار. في حالة نمط تسلسل شفرات الكتل، نستخدم IV تشتمل على قيم صفرية بالكامل، بحيث تنتج C_1 تمامًا مثلما هو الحال مع استخدام نمط كتاب الشفرات الإلكتروني. بناءً عليه، يجري الحصول على C_1 من خلال تدوير $M_1 \oplus K = A \oplus B = 1010 \oplus 1011 = 0001$ للحصول على 0010. إذن، $C_1 = 2$.

لحساب C_2 تُجرى العملية الآتية:

$$M_2 \oplus C_1 = 2 \oplus 2 = 0010 \oplus 0010 = 0000$$

$$0000 \oplus K = 0 \oplus D = 0000 \oplus 1011 = 1011$$

بإجراء عملية التدوير نحصل على $C_2 = 0111 = 7$. لحساب C_3، نحصل على الآتي:

$$M_3 \oplus C_2 = 3 \oplus 7 = 0011 \oplus 0111 = 0100$$

$$0100 \oplus K = 0100 \oplus 1011 = 1111$$

يؤدي إجراء عملية التدوير إلى الحصول على $C_3 = 1111 = F$. لحساب C_4، نحصل على الآتي:

$$M_4 \oplus C_3 = A \oplus F = 1010 \oplus 1111 = 0101$$

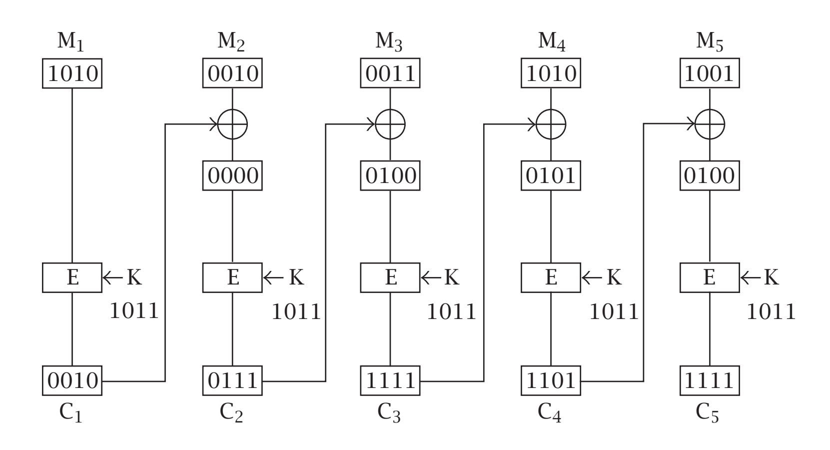
$$0101 \oplus K = 0101 \oplus 1011 = 1110$$

بتنفيذ عملية التدوير نحصل على $C_4 = 1101 = B$. نترك القارئ يحسب قيمة C_5.

بناءً عليه، نحصل على نصين مشفرين من خلال الرسالة نفسها، وهو ما يعتمد على نمط التشفير.

الرسالة:	A 2 3 A 9
النص المشفَّر باستخدام نمط كتاب الشفرات الإلكتروني:	2 3 1 2 4
النص المشفَّر باستخدام نمط تسلسل شفرات الكتل:	2 7 F B F

حتى في مثل هذا المثال البسيط، يبدو من الواضح عدم وجود علاقة مباشرة بين مواضع الكتل المتناظرة في الرسالة ومواضع الكتل المتناظرة في النص المشفر.



رسم يوضح مثال على نمط تسلسل شفرات الكتل.

عند استخدام شفرات الكتل وفق نمط التغذية المرتدة للشفرات، تختلف العملية التي يجري تنفيذها. في المقابل، يتشابه الأثر الناتج؛ وهو ما يعني أن كل كتلة في النص المشفر تعتمد على الكتلة المقابلة لها في النص الأصلي وكل كتلة سابقة لها في النص الأصلي، وذلك وفق الترتيب الذي تظهر به في الرسالة. للمزيد حول نمط التغذية المرتدة للشفرات، انظر كتاب مينيزس، وفان أروشخوت، وفانستون «دليل علم التشفير التطبيقي».

(٣) الاعتماد

هناك معنيان مختلفان لكلمة «اعتماد» في سياق أمن المعلومات. يرتبط أحد هذين المعنيين باعتماد مصدر البيانات، وهو ما يتعلق بالتحقق من أصل البيانات المتلقاة، فيما يرتبط

المعنى الآخر باعتماد هوية (القرين)؛ حيث يجري التحقق من هوية أحد الكيانات من خلال هوية كيان آخر.

يصاحب اعتماد مصدر البيانات، عادةً، عملية تأكيد سلامة البيانات. ويتخذ اعتماد الكيانات أشكالًا متعددة، لكن عندما يقوم على أساس التشفير، فإنه يستند في الغالب إلى تبادل الرسائل بين الكيانَين المتراسلين. يطلق على عملية التبادل هذه اسم «بروتوكول الاعتماد». أشرنا عبر صفحات هذا الكتاب غير مرة إلى المستخدمين واعتبرناهم أشخاصًا، ومع ذلك، في هذا السياق، قد يكون الكيان كمبيوتر أو شخصًا.

بطبيعة الحال، تعتبر عملية اعتماد المستخدم أساسية بالنسبة إلى مفهوم التحكم في الحصول على البيانات، وتوجد طرق عديدة يستطيع المستخدمون من خلالها اعتماد أنفسهم، سواءٌ بعضهم مع بعض، أو مع شبكات الكمبيوتر. وفي الغالب، تعتمد الأساليب الأساسية المستخدمة في عمليات الاعتماد على واحد على الأقل من الخواص الثلاث التالية:

- «شيء معروف»: ربما يكون ذلك — على سبيل المثال — كلمةَ مرورٍ أو رقمَ تعريفٍ شخصيًّا يحتفظ به المستخدم سرًّا.
- «شيء مملوك»: تشمل أمثلة ذلك البطاقات البلاستيكية أو الآلات الحاسبة الشخصية المحمولة.
- «بعض السمات الشخصية للمستخدم»: يشمل ذلك القياسات الحيوية، مثل بصمات الأصابع وبصمات شبكية العين، والإمضاءات المكتوبة يدويًّا، والبصمات الصوتية.

تتضمن أكثر الأساليب شيوعًا المزاوجة على الأرجح بين شيء معروف وشيء مملوك. بطبيعة الحال، يوجد دومًا خطر اكتشاف أي شيء معروف من قِبَل طرف خَصم، وقد يسرق هذا الطرف أو ينسخ أي شيء مملوك. ويعزز ذلك من الزعم القائل بأن الأساليب الوحيدة التي يمكن أن تتحقق من هوية المستخدمين يجب أن تعتمد على خصائص تتعلق بهم، مثل أسلوب «القياس الحيوي». ومع ذلك، لا يجري تطبيق أسلوب القياس الحيوي على نطاق واسع بعدُ لعدة أسباب عملية.

(٤) استخدام الخوارزميات المتناظرة لإجراء الاعتماد والتأكد من سلامة البيانات

يمكن تحقيق الاعتماد والتأكد من سلامة البيانات من خلال استخدام التشفير المتناظر. نتناول أولًا الاعتماد ثم ننتقل للحديث عن سلامة البيانات. يوجد نوعان من الاعتماد. في حالة «الاعتماد في اتجاه واحد»، يجري اعتماد مستخدم بالنسبة إلى مستخدم آخر، وفي حالة «الاعتماد في اتجاهين» يجري اعتماد كلا المستخدمَين أحدهما لدى الآخر. يناقش الفصل التاسع استخدام بطاقة الشرائط الممغنطة في ماكينات الصراف الآلي، وهو أحد أمثلة الاعتماد في اتجاه واحد. يجري اعتماد البطاقة بالنسبة إلى ماكينة الصراف الآلي باستخدام رقم التعريف الشخصي. ومع ذلك يجب على حامل البطاقة استخدام وسائل لا تعتمد على التشفير مثل موضع وتصميم الماكينة للاقتناع بأن الماكينة حقيقية. يعتبر تسجيل البيانات في الكمبيوتر مثالًا آخر على الاعتماد في اتجاه واحد. ويتضمن كلا النوعين من الاعتماد استخدامَ خوارزمية ومعلومات سرية أو مفتاح سري متفق عليها. ويحقق الاستخدام الصحيح لهذا المفتاح في الخوارزمية الاعتمادَ المطلوب. بداهةً، تعتمد هذه العملية على عدم فك شفرة المفتاح. بالإضافة إلى ذلك، تتطلب أساليب الاعتماد المتطورة عادةً استخدام برتوكول متفق عليه يتضمن تبادل أسئلة وإجابات (التي هي في حقيقة الأمر نُسخ مشفرة من الأسئلة).

من الضرورة بمكانٍ الإشارةُ إلى أن استخدام بروتوكول اعتماد يرسِّخ هويات الأطراف ذات الصلة لحظةَ استخدام البروتوكول. في حال الحاجة إلى تحقيق السرية أو التأكد من سلامة البيانات خلال عملية الاتصال التي جرى اعتمادها توًّا، تُستخدم آليات تشفير أخرى لتوفير مثل هذه الحماية. ربما يجري تبادل المفاتيح اللازمة لإجراء عمليات التشفير هذه كجزء من بروتوكول الاعتماد. في المقابل، في حال الحاجة إلى توفير الحماية إزاء محاكاة أحد المحتالين لبروتوكول الاعتماد (أو جزء منه)، يجب استخدام معلومات إضافية مثل أعداد متتالية أو أختام زمنية.

يمكن ضمان سلامة البيانات باستخدام خوارزمية اعتماد ومفتاح سري. وتقبل خوارزمية الاعتماد الرسالة والمفتاح المتفق عليه كمُدخل، ثم تحسب قيمة اعتماد تمثِّل المُخرَج. ولا تعدو قيمة الاعتماد هذه سوى سلسلة أرقام ثنائية (قصيرة) تعتمد قيمتها على خوارزمية الاعتماد، والرسالة، والمفتاح المتفق عليه. باستخدام مصطلحات الفصل الخامس، خوارزمية الاعتماد هي دالة اختزال ذات مفتاح.

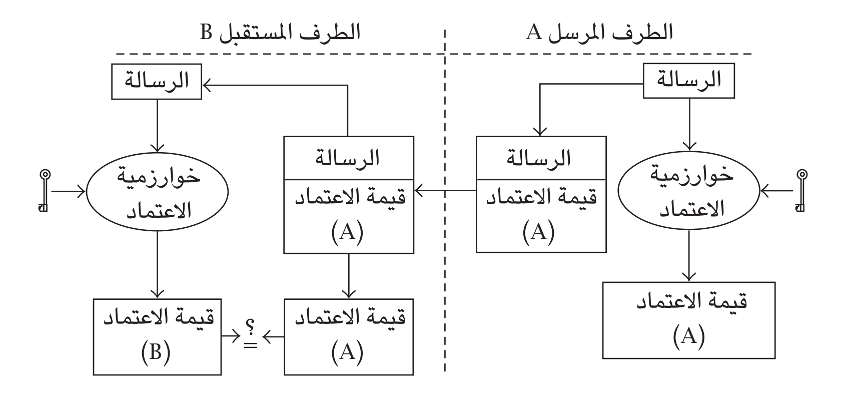
عندما يرغب المستخدم A في إرسال رسالة إلى المستخدم B، يُلحِق قيمة الاعتماد بالرسالة. يتلقى B الرسالة وقيمة اعتمادها. يحسب B بعد ذلك مُخرَج خوارزمية الاعتماد في ضوء الرسالة التي يتلقاها من A والمفتاح السري المتفق عليه كمُدخَل. إذا اتفق هذا المُخرَج مع قيمة الاعتماد التي أرسلها A، يطمئن B إلى أن الرسالة جاءته من A ولم يَجرِ تغييرها. (بناءً عليه، توفر دالة الاعتماد ضمانة للتأكد من سلامة البيانات كما تتحرى من هوية A.) ربما يَلفت نظرَ القارئ القوي الملاحظة أن استخدام هذا النوع من أساليب الاعتماد لا يمنع محاكاة بروتوكول الاعتماد. لتحقيق الحماية ضد هذا النوع من عمليات الاعتراض، مثلما أشرنا، يجب على المستخدمين إلحاق أدوات تعريف، مثل سلسلة من الأعداد، بالرسائل.

يتمثل أحد الجوانب المهمة لعملية الاعتماد هذه في أن كلا الطرفين المرسِل والمستقبِل ينفذان نفس العمليات الحسابية تمامًا. بناءً عليه، إذا كان ثمة نزاع بين A وB حول طبيعة المحتوى الذي جرى تبادله، لا توجد وسيلة تشفيرية لتسوية هذا النزاع. لا يعتبر ذلك خطأ النظام، بل هو نتيجة مترتبة على استخدام التشفير المتناظر. هنا يجب على كلٍّ مِن A وB أن يثق في الآخر. يتشارك A وB في معرفة المفتاح السري كما يعتمدان على سرية ذلك المفتاح لحمايتهما من عمليات الاعتراض لتغيير المحتويات التي يجري تبادلها عن طريق طرف ثالث. ولا يسعى الطرفان إلى تحقيق الحماية كلٌّ منهما إزاء الآخر؛ حيث إنهما يمتلكان ثقة متبادلة. عمومًا، ينطبق هذا الأمر على معظم المستخدمين لنظام التشفير المتناظر الذي يجري استخدامه من قِبَل أطرافٍ بينها ثقة متبادلة لحماية معلوماتها من بقية العالم.

يعتبر أكثر أنظمة الاعتماد استخدامًا، خاصة في القطاع المالي، نظام «رمز اعتماد الرسالة». فإذا كانت الرسالة هي $M_1, M_2, \ldots, M_n$، حيث تتألف كل M_i من 64 رقمًا ثنائيًّا، يُستخدم نظام معيار تشفير البيانات وفق نمط تسلسل كتل الشفرات. ومع ذلك تكون كتلة نص التشفير المطلوبة هي فقط C_n. وهكذا، يتألف نظام شفرة اعتماد الرسالة من 32 رقمًا ثنائيًّا في الكتلة C_n.

(٥) التوقيعات الرقمية

للأسباب التي جرى ذكرها في الفصل الخامس، يميل استخدام الخوارزميات غير المتناظرة إلى الاقتصار على حماية المفاتيح المتناظرة وإلى توفير التوقيعات الرقمية. إذا كان ثمة



الاعتماد من خلال نظام الاعتماد المتناظر.

اشتراط لتسوية النزاعات بين الطرفين، المرسِل والمستقبِل، حول محتويات رسالة ما أو مصدرها، فلا يوفر التشفير المتناظر حلًّا لذلك؛ ومن ثَمَّ يجري اللجوء إلى التوقيعات الرقمية.

يتمثل «التوقيع الرقمي» لرسالةٍ ما جاءت من طرف مرسِل محدد في قيمة مشفرة تعتمد على الرسالة وعلى الطرف المرسل. في المقابل، يعتمد التوقيع المكتوب يدويًّا على الطرف المرسل فقط، وهو لا يختلف في جميع الرسائل. يحقق التوقيع الرقمي سلامة البيانات كما يعتبر دليلًا على المصدر (عدم الإنكار). ويستطيع الطرف المستقبل الاحتفاظ بالتوقيع الرقمي لتسوية النزاعات في حال إنكار الطرف المرسل لمحتوى الرسالة أو حتى إنكاره لقيامه بإرسالها. يعتبر التوقيع الرقمي وسيلة لتسوية النزاعات بين الطرفين المرسل والمستقبل، وهي طريقة تتميز بها آلية التوقيع الرقمي عن عملية الاعتماد من خلال نظام رمز اعتماد الرسالة الذي جرى مناقشته في الجزء السابق. بداهةً، لا يمكن تسوية هذا النوع من النزاعات إلا في حال وجود حالة عدم تماثل بين الطرفين المرسل والمستقبل. توحي هذه الملاحظة بأن أنظمة التشفير غير المتناظر تعتبر الأدوات المعتادة لتوفير التوقيعات الرقمية.

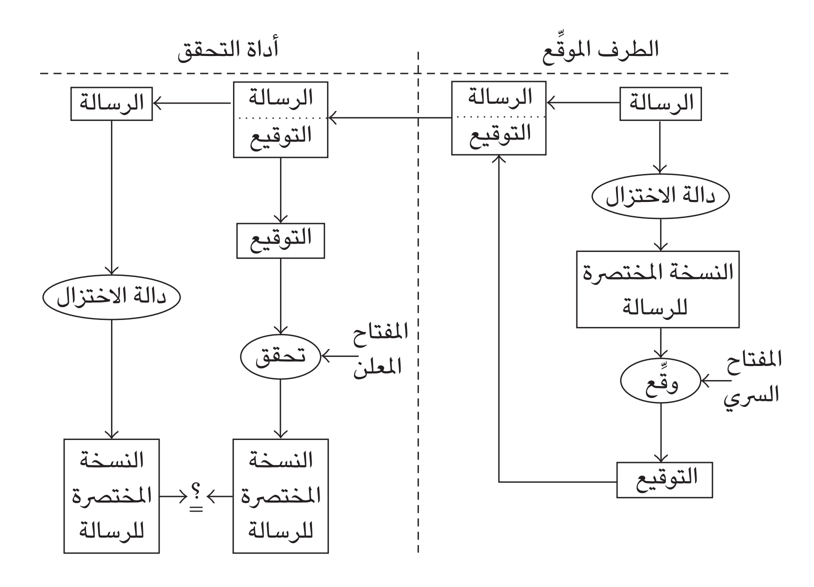
المبدأُ الرئيسي في تصميم توقيع رقمي يعتمد على نظام مفاتيح معلنة مثل نظام آر إس إيه أو نظام الجَمَل؛ بسيطٌ جدًّا. يمتلك كل مستخدم مفتاحًا سريًّا لا يستطيع

أي شخص آخر استخدامه، ويُستخدم المفتاحُ كوسيلة لتحديد هويته. في المقابل، يوجد مفتاح معلن مقابل. وفي حين يستطيع كلٌّ مَن يعرف هذا المفتاح المعلن التأكد من أن المفتاح السري المقابل له جرى استخدامه، فإنه لا يستطيع تحديد المفتاح السري.

التسليم بأن المفتاح السري لا بد أن يكون قد جرى استخدامه، يعطي الطرف المستقبل ثقة في مصدر ومحتوى الرسالة. في المقابل، يتأكد الطرف المرسل أنه يستحيل حدوث عملية انتحال للهوية؛ نظرًا لأن المفتاح السري أو مفتاح «التوقيع» لا يمكن استنباطه من خلال المفتاح المعلن أو مفتاح «التحقق» أو التوقيع الرقمي.

تتطلب عملية التشفير غير المتناظر الكثير من عمليات المعالجة الحاسوبية. بناءً عليه، يجري توليد نسخة مضغوطة أو مختصرة للرسالة من خلال تطبيق دالة الاختزال على الرسالة. يجري توليد التوقيع من النسخة المختزلة (التي تمثل الرسالة) من خلال استخدام الخوارزمية غير المتناظرة مع المفتاح السري. بناءً عليه، لا يتمكن أحد سوى مالك المفتاح السري من توليد التوقيع. يمكن التحقق من التوقيع عن طريق أي طرف يعرف المفتاح المعلن المقابل. لإجراء ذلك، يجري توليد قيمة من خلال التوقيع باستخدام الخوارزمية غير المتناظرة مع المفتاح المعلن، وهي قيمة تكافئ قيمة النسخة المختزلة للرسالة التي يستطيع أي شخص حسابها. إذا تطابقت هذه القيمة مع صيغة الرسالة المختصرة، يجري قبول صحة التوقيع، وفي حال عدم التطابق، يعتبر التوقيع غير صحيح.

أكثر الخوارزميات غير المتناظرة استخدامًا خوارزميةُ آر إس إيه وخوارزمية الجَمَل. في حالة خوارزمية آر إس إيه، تتطابق عمليتا التشفير وفك التشفير؛ لذا تتطابق عمليتا تصميم التوقيع والتحقق منه أيضًا. ويتمثل أحد بدائل خوارزمية آر إس إيه في معيار التوقيع الرقمي، الذي يعتمد على خوارزمية الجمل. ففي حالة خوارزمية التوقيع الرقمي، تختلف عمليتا التوقيع والتحقق. بالإضافة إلى ذلك، تتطلب خوارزمية التشفير الرقمي مولد أعداد عشوائية (وهو ما يتطلب إجراء المزيد من العمليات)، بينما لا تتطلب خوارزمية آر إس إيه ذلك. في المقابل، بينما يصدر عن خوارزمية التوقيع الرقمي دومًا توقيعٌ ثابت طوله 320 رقمًا ثنائيًّا، في حالة خوارزمية آر إس إيه يكون لكلٍّ مِن كتلة التوقيع والمقياس الحسابي نفس الحجم، الذي يزيد مع زيادة مستوى الأمن في النظام.



التوقيعات الرقمية.

هب أن التوقيعات الرقمية يجري استخدامها كوسيلة للتعريف؛ إذا كان المستخدم A يرغب في انتحال شخصية المستخدم B، يوجد شكلان مختلفان لإجراء عملية الاعتراض:

(١) يحاول A استخدام مفتاح B السري.
(٢) يحاول A الاستعاضة عن مفتاحه المعلن بمفتاح B المعلن.

تتضمن عمليات الاعتراض من النوع الأول محاولة فك شفرة الخوارزمية أو اختراق الأجهزة التي تحتوي على المفتاح السري. جرت مناقشة عمليات اعتراض الخوارزميات في الفصل السادس، بينما تعتبر الحاجة إلى تحقيق أمن للأجهزة سمة مهمة من سمات إدارة المفاتيح، وهو موضوع الفصل الثامن. يشبه نوعَا الاعتراض هنا أنواع الاعتراض التي تستهدف الأنظمة المتناظرة. ومع ذلك تعتبر عمليات الاعتراض من النوع الثاني فريدة في حالة أنظمة المفاتيح المعلنة. تتضمن معظم «العمليات الدفاعية» الحالية استخدام الشهادات الرقمية التي تصدرها جهات الاعتماد.

(٦) جهات الاعتماد

ناقشنا توًّا عمليات الاعتراض «التقليدية» التي تستهدف أنظمة التشفير، مثل فك شفرة الخوارزمية لتحديد المفتاح السري، أو الحصول على المفتاح السري من خلال اختراق الأجهزة، مثل امتلاك جهاز يمكِّن من استخدام المفتاح أو اختراق الأجهزة الأخرى لقراءة القيمة السرية. ومع ذلك تحتاج أنظمة المفاتيح المعلنة إلى بنية تحتية للحيلولة دون وقوع عمليات انتحال هوية. هب أن المستخدم A استطاع تصميم مفتاحه المعلن باعتباره يخص المستخدم B؛ بناءً عليه، سيستخدم المستخدمون الآخرون مفتاح A المعلن لتشفير المفاتيح المتناظرة لصالح B. وهكذا، يحصل A، بدلًا من B على المعلومات السرية المحمية عن طريق هذه المفاتيح المتناظرة. بالإضافة إلى ذلك، سيستطيع A توقيع الرسائل باستخدام مفتاحه السري، وهي التوقيعات التي ستُقبل على أنها تخص B. يهدف استخدام جهات الاعتماد وإنشاء بنية تحتية للمفاتيح المعلنة إلى الحيلولة دون وقوع حالات انتحال كهذه.

يتمثل الدور الرئيسي «لجهة الاعتماد» في توفير «شهادات» موقعة رقميًّا يجري من خلالها ربط هوية أحد الكيانات بقيمة مفتاحه المعلن. وللتحقق من شهادات جهة الاعتماد، يجب أن يكون المفتاح المعلن لجهة الاعتماد معروفًا ومقبولًا على نطاق واسع. بناءً عليه، في هذا السياق، تعتبر الشهادة رسالة موقعة تحتوي على هوية الكيان، وقيمة مفتاحه المعلن، وربما بعض المعلومات الإضافية مثل تاريخ انتهاء الشهادة. يمكن النظر إلى هذه الشهادات باعتبارها «خطاب تعارف» من مصدر يتمتع بالاحترام (جهة الاعتماد).

هب أن سي إي آر تي إيه شهادة تصدرها جهة الاعتماد، تحتوي على هوية المستخدم A ومفتاحه المعلن؛ تربط سي إي آر تي إيه، إذن، بين هوية A وقيمة مفتاحه المعلن، يستطيع كلُّ مَن يمتلك نسخة صحيحة من المفتاح المعلن لجهة الاعتماد التحققَ من أن التوقيع في شهادة سي إي آر تي إيه هو توقيع صحيح؛ ومن ثَمَّ يطمئن إلى معرفة المفتاح المعلن للمستخدم A. بناءً عليه، يحل محل مشكلة ضمان حقيقة المفتاح المعلن للمستخدم A مشكلة الحاجة إلى ضمان كون المفتاح المعلن لجهة الاعتماد صحيحًا، فضلًا عن الثقة في أن عملية التحقق من هوية A جرى تنفيذها على نحو صحيح. لاحظ أن كلَّ مَن يستطيع انتحال شخصية A خلال عملية الاعتماد يستطيع الحصول على شهادة تربط مفتاحه المعلن بهوية A، وهو ما يمكِّنه من انتحال هوية A خلال دورة

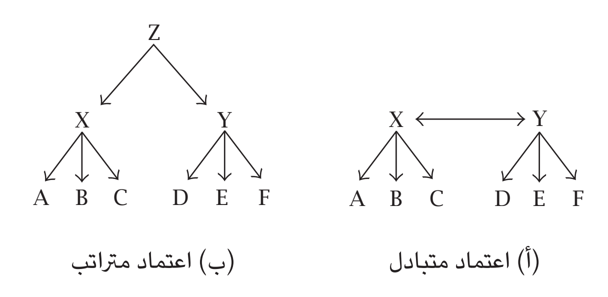
الحياة الكاملة للشهادة. يعتبر ذلك مثالًا على مشكلة سرقة الهوية المثيرة للقلق، وهي مشكلة مرشحة للزيادة في المستقبل.

من الأهمية بمكان ملاحظة أن أي شخص قد يستطيع إصدار شهادة أحد المستخدمين؛ بحيث لا يعبِّر امتلاك الشهادة الرقمية للمستخدم A عن هوية A. تربط الشهادة فقط بين هوية A وقيمة المفتاح المعلن. يمكن البرهنة على هوية المستخدم، إذن، من خلال استخدام بروتوكول أسئلة-أجوبة يثبت استخدام مفتاح A السري، وهو ما قد يتضمن تقديم طلب توقيع إلى A. يجيب A الطلب بإدخال توقيعه، ثم تُؤكد أداة التحقق صحة التوقيع من خلال استخدام قيمة المفتاح المعلن في شهادة A. ولا يثبت هوية A سوى استخدام المفتاح السري المقابل للمفتاح المعلن في شهادة A.

هب أن مستخدمَيْن، A وB، صدرت لهما شهادتان من جهتي اعتماد مختلفتين؛ إذا أراد A ضمان صحة مفتاح B المعلن، فإنه سيحتاج إلى نسخة صحيحة من مفتاح B المعلن في شهادة جهة الاعتماد. يتحقق ذلك من خلال عملية «اعتماد متبادل»، تصدر جهتا الاعتماد من خلالها شهادة تعتمد فيها شهادة الجهة الأخرى؛ أو من خلال «الاعتماد المتراتب»، ترأس فيها جهة اعتماد رئيسية جهتي الاعتماد وتصدر شهادة إلى كلٍّ منهما.

يبيِّن الشكلان عمليتين. في كل حالة، تشير X وY إلى جهتَيِ اعتماد بينما تشير A → X إلى أن X تصدر شهادة إلى A. في (ب) تعتبر Z جهة اعتماد رئيسية. على سبيل المثال، إذا أراد B التحقق من مفتاح E المعلن، إذن، فبالنسبة إلى الحالة (أ) سيحتاج B إلى التحقق من شهادة Y التي أصدرتها X وشهادة E التي أصدرتها Y. بالنسبة إلى الحالة (ب)، يحتاج B إلى التحقق من شهادة Y التي أصدرتها Z وشهادة E التي أصدرتها Y. بناءً عليه، في كل حالة، يحتاج B إلى تحري سلسلة تتألف من شهادتين. تطول هذه السلسلة كثيرًا في حالات الأنظمة الأكثر تعقيدًا التي تتضمن مزيجًا يتألف من أكثر من عملية اعتماد متبادلة واعتماد متراتب على أكثر من مستوًى.

ينظر الكثيرون إلى التوقيعات الرقمية كأدوات في غاية الأهمية في التجارة الإلكترونية، فيما يقترح العديد من البلدان تشريعات تحصل من خلالها التوقيعاتُ الرقمية على الوضع القانوني نفسه الذي تتمتع به التوقيعات اليدوية. لمطالعة عرض شامل وحديث لآليات



(ب) اعتماد متراتب (أ) اعتماد متبادل

التوقيع الرقمي والاطلاع على عرض للموضوعات المصاحبة للبِنى التحتية للمفاتيح المعلنة، نُحيل القارئ إلى كتاب بايبر، بليك-ويلسون، وميتشل، «التوقيعات الرقمية». ومع ذلك توجد بعض الموضوعات المهمة جدًّا يجب التطرق إليها هنا. إحدى المشكلات الرئيسية المصاحبة لاستخدام الشهادات هي مشكلة «الإلغاء». ومن الأمثلة على ذلك إصدار شركةٍ شهادةً إلى أحد الموظفين الذي يترك الشركة لاحقًا. يوجد مثال آخر وهو حامل مفتاح على دراية بانكشاف مفتاحه السري. في كلتا الحالتين، يجب توفر شرط قدرة جهة الاعتماد على إلغاء الشهادة. وبما أن هذه الشهادات جرى توزيعها على الأرجح على نطاق واسع، فمن الصعب عمليًّا إخطار الجميع بإلغائها. يتمثل أحد حلول التغلب على ذلك في نشر جهة الاعتماد قائمة الشهادات الملغاة. ومع ذلك يعتبر هذا عبئًا إداريًّا ثقيلًا، فضلًا عن وجود مشكلات كثيرة مصاحبة له.

تتعلق مشكلة أخرى في استخدام الشهادات بتحديد المسئولية؛ حيث سيعتمد كثير من المستخدمين على هذه الشهادات. هب أن شهادة منها كانت غير صحيحة؛ وهو ما يعني عدم انتماء قيمة المفتاح المعلن بها إلى المالك الحقيقي المدرج؛ في هذه الحالة، لا يبدو واضحًا على أيٍّ من الأطراف تقع المسئولية: المالك، أم المستخدم، أم جهة الاعتماد.

(٧) البنية التحتية للمفاتيح المعلنة

يكمن دافع إنشاء بنية تحتية للمفاتيح المعلنة في تيسير تنفيذ عملية التشفير بالمفتاح المعلن. في كتاب آدمز ولويد، «فهم البنية التحتية للمفاتيح المعلنة»، الذي كان حسب معلوماتنا، الكتابَ الأول من نوعه حول الموضوع، وُضع تعريف للبنية التحتية للمفاتيح

المعلنة كالآتي: «بنية تحتية أمنية شاملة يجري تنفيذ وتقديم خدماتها باستخدام مفاهيم وأساليب المفاتيح المعلنة.»

أكدنا على أهمية عملية تحقيق الهوية، والحاجة إلى توفر القدرة على إلغاء الشهادات، ومفهوم الاعتماد المتبادل. بديهيًّا، ستعتبر عملية الاعتماد المتبادل في غاية الصعوبة ما لم تَستخدم جهاتُ الاعتماد تكنولوجياتٍ مناسبة. حتى في حال استخدام مثل هذه التكنولوجيات، لا يزال يوجد عدد من المشكلات المصاحبة للمشكلة العامة المتعلقة بكيفية تحديد المستخدمين أيُّ شهادات جهات الاعتماد يمكنهم الوثوق بها. بناءً عليه، يجب على جهات الاعتماد نشر بيانات سياسات وممارسات تتضمن، فيما تتضمن من معلومات، عباراتٍ واضحةً حول إجراءاتها الأمنية.

حتى الآن، جرى تحديد ثلاثة لاعبين رئيسيين في نظام البنية التحتية للمفاتيح المعلنة؛ ألا وهم: مالك الشهادة، الذي يتقدم بطلب الحصول عليها؛ وجهة الاعتماد، التي تصدر الشهادة التي تربط بين هوية المالك وقيمة المفتاح المعلن للمالك؛ والمستخدم الذي يستخدم الشهادة ويعتمد عليها. في بعض الأنظمة، يجري تنفيذ عملية التحقق من الهوية من خلال جهة منفصلة يطلق عليها اسم «جهة التسجيل».

مثلما رأينا، في بنية تحتية ضخمة تتضمن عددًا كبيرًا من جهات الاعتماد، قد تتضمن العملية، التي يتحقق من خلالها مستخدمٌ ما من المفتاح المعلن لمستخدم آخر، التحققَ من توقيعات في سلسلة طويلة من الشهادات، وهو ما يعد أمرًا مكلفًا، كما يستغرق وقتًا طويلًا للغاية؛ ومن ثَمَّ قد لا يرغب المستخدمون في القيام به. ظهر مفهوم «جهة التحري» لتوفير عبء تنفيذ ذلك على المستخدمين. تتمثل الفكرة الأساسية في أن المستخدمين النهائيين يطلبون من جهة التحري التحققَ من صحة إحدى الشهادات ثم تَلَقِّيَ إجابة بنعم أو لا. ينتقل جهد التحري إذن من المستخدم إلى جهة التحري.

بينما تعتبر البِنى التحتية للمفاتيح المعلنة والتوقيعات الرقمية أكثر مجالات التشفير ارتباطًا حاليًّا بالتجارة الإلكترونية، يبدو أن الراغبين في تطبيقها يواجهون عددًا من المشكلات الفنية في التطبيق، مثل المشكلات المصاحبة لمسألة جاهزية نظام العمل لارتفاع الطلب. بالإضافة إلى ذلك، على الرغم من وجود مزاعم تشير إلى الأهمية البالغة لتكنولوجيا البنية التحتية للمفاتيح المعلنة لتوفير الأمن في حسابات البريد الإلكتروني، والاتصال بالخوادم الشبكية، والشبكات الافتراضية الخاصة؛ ثبت أن الحافز التجاري الذي يدفع مؤسسةً ما إلى تأسيس كيان يمارس دور جهة الاعتماد أقل جاذبية بكثير من المتوقع.

عند تأسيس بنية مفاتيح معلنة تحتية، يجب إجراء العمليات التالية، دون الالتزام بترتيب إجرائها:

- يجب توليد زوجَيْ مفاتيح جهات الاعتماد.
- يجب توليد زوجَيْ مفاتيح المستخدمين.
- يجب على المستخدمين طلب شهادات.
- يجب التحقق من هوية المستخدمين.
- يجب التحقق من زوجَيْ مفاتيح المستخدمين.
- يجب إصدار شهادات اعتماد.
- يجب التأكد من صحة الشهادات.
- يجب إزالة/تحديث الشهادات (متى كان ذلك لازمًا).
- يجب إلغاء الشهادات (متى كان ذلك لازمًا).

تتمثل الأسئلة الأساسية المتعلقة بهذه العمليات في سؤالَيْن هما «أين؟» و«عن طريق مَن؟» تُصدر بعض جهات الاعتماد شهادات تتضمن «مستويات» مختلفة مرفقة بها؛ حيث يشير المستوى إلى درجة الثقة في الشهادات. على سبيل المثال، يُنصح المستخدمون بعدم الاعتماد على شهادات منخفضة المستوى عند إجراء معاملات بمبالغ مرتفعة. في هذه الأنظمة، يعكس مستوى الشهادة على الأرجح كيفية إجراء عملية التثبت من الهوية. على سبيل المثال، إذا جرى التحقق من هوية المستخدم من خلال استخدام عنوان البريد الإلكتروني، فستكون الشهادة الصادرة منخفضة المستوى، بينما تصدر الشهادات مرتفعة المستوى فقط عند إجراء عملية يدوية تتضمن تقديم المستخدم لجواز سفره. للاطلاع على عرض شامل جيد للمشكلات المصاحبة للبنية التحتية للمفاتيح المعلنة والحلول الممكنة لها، نُحيل القارئ إلى كتاب آدمز ولويد، «فهم البنية التحتية للمفاتيح المعلنة»، أو كتاب كلابرتون، «دليل التجارة الإلكترونية».

(٨) الحاجة إلى الثقة

تقدِّم جهات الاعتماد مثالًا على مفهوم «الطرف الثالث الموثوق به». في هذه الحالة، يثق طرفان في طرف ثالث — جهة الاعتماد — ثم يعتمدان على هذه الثقة في إجراء عمليات اتصال آمنة بينهما. تظهر الأطراف الثلاثة الموثوق بها تقريبًا في كل مجال يستخدم فيه

التشفير، ويشكِّل الاعتماد عليها مصدرًا للقلق. فبوجه عام، هناك حاجة إلى الثقة في هذه الأطراف من ناحية نزاهتها وكفاءتها الفنية. ومن الصعوبة بمكان في كثير من الأحيان تحديد مدى تأثيرها على وجه الدقة، فضلًا عن قدر اعتماد أمن المستخدمين عليها.

تدبرْ — على سبيل المثال — إجراء عملية توليد زوج مفتاح معلن ومفتاح سري؛ مثلما أشرنا، تعتبر هذه العملية عملية رياضية تشترط توافر برامج خاصة لإجرائها. وبما أن هذه العملية لا يستطيع المستخدم العادي إجراءها بنفسه، لذا يجري توفير برامج تصميم المفاتيح أو توليد المفاتيح خارجيًّا. في كلتا الحالتين، توجد حاجة ملحة إلى توفر حالة من الثقة. يجري كثيرًا توليد المفاتيح خارجيًّا. والسؤال البديهي هنا هو: هل كان يجب توليد المفاتيح عن طريق جهة الاعتماد أو عن طريق طرف ثالث آخر موثوق به؟ وفي حين أننا لا نسعى هنا إلى تقديم إجابة، إذ إن ذلك يعتمد بوضوح على كلٍّ مِن التطبيق والسياق، نرمي إلى لفت الانتباه إلى بعض الموضوعات المطروحة. يتمثل الهاجس في هذه الحالة في أنه في حال توليد إحدى المؤسسات لزوج المفتاحين المعلن والسري لكيان آخر، ربما تحتفظ هذه المؤسسة بنسخة من المفتاح السري أو تكشف عنه لأطراف أخرى. لا ينتهي الجدال حول هذه المسألة، بل يرى البعض عدم ضرورة وجود جهة اعتماد على الإطلاق.

في عام ١٩٩١، طُرحت النسخة الأولى من مجموعة برامج «خصوصية آمنة تمامًا» مجانًا لكل مَن أراد استخدام تشفير قوي. استَخدمتْ هذه البرامج نظام تشفير آر إس إيه للتحقق من هوية المستخدمين ولإجراء عملية توزيع متناظرة للمفاتيح، كما استخدمت خوارزمية تشفير متناظرة باسم آي دي إي إيه لتحقيق السرية. وعلى الرغم من استخدام الشهادات الرقمية ضمن هذه البرامج، لم تعتمد النسخة الأولى من هذه البرامج على وجود جهة اعتماد مركزية. بدلًا من ذلك، قد يلعب المستخدم دور جهة الاعتماد بالنسبة إلى أي مستخدم آخر، وهو ما صار يُعرف باسم أسلوب «شبكة الثقة». تعتمد فكرة شبكة الثقة في الأساس على إصدار المستخدمين أحكامًا حيال مدى موثوقية أي شهادة بناءً على ما إذا كان قد جرى توقيعها عن طريق طرف يثقون فيه أم لا. في حالة شبكات الاتصال الصغيرة، لا تعدُّ هناك حاجة عند استخدام مثل هذا الأسلوب إلى وجود جهة اعتماد مركزية، وقد يحقق هذا الأسلوب نجاحًا. بيد أنه يوجد عدد من المشكلات المحتملة في حالة الشبكات الكبيرة.

ثمة بديل آخر من أجل التخلص من الحاجة إلى وجود جهة اعتماد؛ وهو أن تحدد هوية المستخدم قيمة مفتاحه المعلن تحديدًا تامًّا. وفي حالِ تَماثَلَتْ هوية أحد المستخدمين (جوهريًّا) مع المفتاح المعلن، فمن الواضح أنه لن تكون هناك حاجة إلى الحصول على شهادات للربط بين الهوية والمفتاح المعلن. كان شامير قد اقترح مفهوم نظام تشفير المفاتيح المعلنة المعتمد على تحقيق الهوية في عام ١٩٨٤، وكان هناك عدد من تصميمات التوقيعات الرقمية يعتمد على هذا المفهوم. في المقابل، لم تصدر خوارزمية المفاتيح المعلنة المعتمدة على الهوية إلا في عام ٢٠٠١. يوجد حاليًّا نسختان من هذه الخوارزمية: نسخة ابتكرها بونيه وفرانكلين، وأخرى صُممت في مجموعة أمن الاتصالات-الإلكترونيات (سي إي إس جي) في المملكة المتحدة.

في الأنظمة المعتمدة على الهوية، يجب توفر جهة مركزية موثوق بها تجري عملية حساب المفتاح السري المقابل للمفتاح المعلن لكل مستخدم ثم تسليمه له. ولا يترتب على هذا الأسلوب، إذن، التخلص من الحاجة إلى طرف ثالث موثوق به، وهو الطرف المسئول عن توليد المفتاح السري لكل مستخدم. ومع ذلك يزيل هذا الأسلوب الحاجة إلى الشهادات. في هذه الحالة، لا توجد ميزة في أن ينتحل المستخدم A شخصية المستخدم B؛ إذ إن B وحده يملك المفتاح السري الذي تحدده هوية B.

يمثل استخدام الأنظمة المفاتيح المعلنة المعتمدة على الهوية بديلًا مثيرًا لأسلوب البنية التحتية للمفاتيح المعلنة التقليدي. لسوء الحظ، لاستخدام هذه الأنظمة مشكلاته، ربما كان أكثرها بداهةً ما يتعلق بمفهوم الهوية الفريدة وبإلغاء المفاتيح المعلنة. هب أن اسم وعنوان المستخدم يحددان مفتاحه المعلن؛ في حال اختراق مفتاحه السري، يجب عليه تغيير عنوانه أو اسمه، وهو ما لا يُعد حلًّا عمليًّا. توجد حلول لمشكلة «سرقة الهوية» هذه. يتمثَّل أحد هذه الحلول في جعل المفتاح المعلن للمستخدم يعتمد على هويته ومتغير آخر معروف، مثل التاريخ. يضمن ذلك تغيير المفتاح السري للمستخدم يوميًّا، لكنه يشكِّل عبئًا كبيرًا على جهة الاعتماد. تُجرى حاليًّا العديد من الأبحاث للنظر فيما إذا كانت هناك سيناريوهات يمكن فيها استخدام أنظمة تعتمد على الهوية لتحل محل أنظمة البنية التحتية للمفاتيح المعلنة.

وعلى النقيض تمامًا، هناك من يرى أن أفضل سبيل لتحقيق الأمن يتمثل في التركيز على أكبر قدر ممكن من المخاطر عند موضع واحد، ثم توفير أقصى حماية ممكنة عنده. إذا جرى تبنِّي هذا الأسلوب، فقد تولِّد جهة الاعتماد مفاتيح المستخدمين. غالبًا ما يذهب

البعض إلى أنه في حال وثوق المستخدم في جهة الاعتماد بما يكفي لتوليد مفتاحه المعلن، سيثق أيضًا في إدارتها مفاتيحه المعلنة نيابةً عنه. يرجع ذلك إلى أن عملية توليد المفاتيح تحتاج إلى البيئة التي تتميز بالأمن الشديد التي توفرها جهة الاعتماد، وهو ما يعرف باسم الأسلوب «المتمحور حول الخادم» الذي ترى فيه جهات معينة حلًّا مناسبًا.

الفصل الثامن

إدارة المفاتيح

(١) مقدمة

في الفصول الأولى، ركَّزنا على الخوارزميات واستخداماتها. ومع ذلك شددنا مرارًا وتكرارًا على أهمية الإدارة الجيدة للمفاتيح. عمومًا، تعتمد كفاءة خدمات التشفير على عدد من العوامل التي تشمل قوة الخوارزمية، وعدد من الخواص المادية، بما في ذلك مقاومة التلاعب بالأجهزة الحيوية والتحكم في استخدام الأجهزة، فضلًا عن إدارة المفاتيح. وتُستخدم الخوارزميات القوية في منع الأطراف المعترضة من حساب المفاتيح. ومع ذلك تتناقص أهمية هذه الخوارزميات في حال قدرة الأطراف المعترضة على الحصول على المفاتيح المناسبة بطرق أخرى. إنَّ أَمْنَ أيِّ نظامِ تشفيرٍ يعتمد كلية على أمن المفاتيح. يجب حماية المفاتيح خلال جميع مراحل دورة حياتها. في هذا الفصل، نشرح بالتفصيل ما نعنيه بإدارة المفاتيح، ونعرض المخاطر التي تتعرض لها المفاتيح، مع مناقشة بعض الحلول العملية. نشير في كثير من الأحيان في هذا الفصل إلى بعض المعايير التي يشيع الاعتماد عليها، خاصةً تلك التي يُصدرها معهد المعايير القومي الأمريكي للقطاع المصرفي. يجب انتقاء أنظمة إدارة المفاتيح بعناية حتى تصبح فعَّالة لضمان تلبية احتياجات الأعمال واشتراطات تنفيذ النظام. ويجب في جميع الأحوال تذكُّر أن أنظمة الأمن التشفيرية المحكمة أكثر من اللازم تمثِّل عبئًا على العمل.

(٢) دورة حياة المفاتيح

يتمثل الهدف الرئيسي لإدارة المفاتيح في الحفاظ على سرية وسلامة جميع المفاتيح في جميع الأوقات. بالنسبة إلى أي مفتاح، تبدأ هذه الدورة بعملية توليد المفتاح ولا تنتهي

إلا بانتهاء استخدام المفتاح وتدميره. يبين الشكل التالي المراحل الرئيسية في دورة حياة المفتاح.

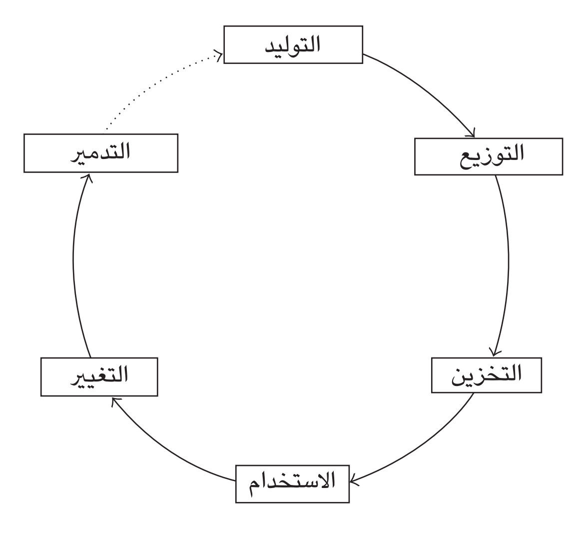
في جميع الحالات تقريبًا، يحل محل كل مفتاح مفتاحٌ آخر. بناءً عليه، تمثل عملية الإحلال دورة؛ وهو ما يعني أن عملية تدمير المفتاح يتلوها عملية الإحلال بمفتاح جديد. لكن هذا المفتاح الجديد يكون، على الأرجح، قد جرى توليده، وتوزيعه، وتخزينه قبل تدمير المفتاح القديم. في بعض الأنظمة، قد تكون هناك اشتراطات إضافية لأرشفة المفاتيح.

ثمة حاجة إلى إجراءات متابعة خلال دورة حياة أي مفتاح، وذلك بغرض اكتشاف عمليات الاعتراض المحتملة له. ويتضمن ذلك بالتأكيد إجراء نوع من تتبُّع أو مراجعة المسار لتسجيل استخدامات المفتاح، ولكن من الواضح أنه لا تتحقق أي فائدة مِن تتبع المسار في حال عدم متابعته. بالإضافة إلى ذلك، تتناقص أهمية عملية المتابعة كثيرًا إلا إذا كان أحدهم يمتلك سلطة التصرف حيال وجود تهديد محتمل يستهدف اكتشاف المفتاح. بناءً عليه، يفضَّل عادةً — خاصة في حالة الأنظمة الكبيرة — وجود مالكين محددين للمفاتيح يتولَّوْن مسئولية حمايتها.

ننتقل الآن إلى تناول كل عنصر من عناصر دورة حياة المفتاح. على الرغم من تطابق كثير من مبادئ الإدارة الأساسية، تختلف إدارة مفاتيح أنظمة التشفير المتناظرة كثيرًا عن إدارة مفاتيح أنظمة التشفير غير المتناظرة. في حقيقة الأمر، يعتبر إنشاء بنية تحتية للمفاتيح المعلنة الأساسَ في بعض سمات إدارة مفاتيح الخوارزميات غير المتناظرة. نركِّز في تناولنا هنا على الأنظمة المتناظرة ونشير إلى بعض التعليقات في حال وجود اختلاف جوهري بين النظامين.

(٢-١) توليد المفاتيح

غالبًا ما تُمثِّل عملية توليد المفاتيح مشكلة، خاصةً في حالة خوارزميات المفتاح المعلن التي تمتلك فيها المفاتيح خواص رياضية معقدة. بالنسبة إلى معظم الخوارزميات المتناظرة، تعتبر أي سلسلة من الأرقام (أو أحيانًا، أي رموز أخرى) بمنزلة مفتاح، وهو ما يشير ضمنًا إلى أن معظم مستخدمي الخوارزميات المتناظرة يمتلكون القدرة على توليد مفاتيحهم. تتمثل المشكلة الرئيسية في توليد المفاتيح بطريقة تجعلها غير قابلة للتنبؤ بها. تشمل الطرقُ الشائعة الأساليبَ اليدوية (مثل قذف العملات المعدنية)،



دورة حياة المفتاح.

اشتقاق المفاتيح من بيانات شخصية (رقم التعريف الشخصي) أو مولد (شبه) عشوائي للأعداد.

يختلف الوضع في حالة الأنظمة غير المتناظرة؛ إذ يتطلب توليدُ أعداد أولية كبيرة إجراءَ بعض العمليات الرياضية المعقدة، وهو ما قد يتطلب توافر موارد ضخمة. مثلما ذكرنا في القسم السابق، ربما يُضطر المستخدِمون إلى الثقة في مفاتيحَ جرى توليدها من قِبل طرف خارجي أو من خلال برامج صاغها طرف خارجي. إذا نظرنا إلى نظام آر إس إيه، فسنجد أن تحقيق الأمن فيه يعتمد على قدرة الطرف المعترض على اكتشاف العوامل الأولية للمقياس الحسابي N. وإذا أسفرت عملية توليد المفتاح عن عدد محدود من الأعداد الأولية، فربما يستطيع الطرف المعترض توليد هذا العدد المحدود من الأعداد الأولية ثم يجرِّب كلَّ عدد أولي كأحد عوامل العدد N. ويعد ذلك مثالًا بسيطًا على أهمية توفر عملية توليد جيدة في أنظمة المفاتيح المعلنة.

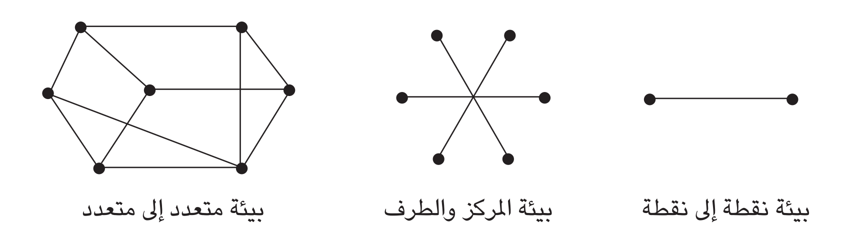
(٢-٢) توزيع وتخزين المفاتيح

تعتبر عمليتا تخزين وتوزيع المفاتيح في غاية الأهمية، وغالبًا ما تكون المشكلاتُ التي تجري مواجهتها والحلول التي يجري تنفيذها لحل هذه المشكلات متشابهةً؛ ومن ثَمَّ نناقشهما معًا.

يرجع السبب في استخدام خوارزمية قوية إلى منع الأطراف المعترضة من حساب المفتاح. لا توجد أي فائدة في خوارزمية قوية إذا استطاعت الأطراف المعترضة اكتشاف المفتاح بطريقة مباشرة في مكانٍ ما من النظام. وغالبًا ما تتضمن عملية تخزين مفاتيح معينة بعض صور الحماية المادية. على سبيل المثال، قد تخزَّن المفاتيح في مواضع يجري التحكم فيها ماديًّا بصرامة، وهو ما سيجعل حماية المفاتيح تعتمد فقط على فعالية أساليب التحكم في الوصول إليها. وكبديل عن ذلك، قد تخزَّن المفاتيح في جهاز مثل بطاقة ذكية تتضمن مستويين للحماية؛ أولًا: يتحمل مالِكو المفاتيح مسئولية ضمان الحفاظ على البطاقة في حوزتهم. ثانيًا: قد تحتوي البطاقة على أسلوب حماية مقاوِم للتلاعب؛ وذلك للحيلولة دون قراءة محتوياتها في حال الحصول عليها.

تتمثل إحدى القواعد الأساسية لحماية المفاتيح في عدم ظهور المفاتيح بوضوح في أي مكان في النظام إلا إذا كانت تتمتع بحماية مادية كافية. وفي حالة عدم توافر الحماية المادية، يجب تشفير المفاتيح باستخدام مفاتيح أخرى أو تقسيم المفاتيح إلى مكونَيْن أو أكثر. جرى اقتراح هذه القاعدة في حين كانت معظم عمليات التشفير تجري في الأجهزة. في حالة إمكانية تنفيذها عمليًّا، لا تزال الحماية المادية ممارسة سليمة؛ إذ يجري النظر إلى التخزين المادي للبيانات باعتباره عمليةً توفِّر حماية أكثر من البرامج. يقود مفهوم حماية المفاتيح من خلال تشفيرها باستخدام مفاتيح أخرى إلى مفهوم «المفتاح الهرمي»؛ حيث يستخدم كل مفتاح في حماية المفتاح الذي يقع أسفله في السلسلة الهرمية. تعتبر السلسة الهرمية للمفاتيح مهمة، وهو ما سنناقشه لاحقًا في هذا الفصل. بَيْد أننا نكتفي بالإشارة في الوقت الحالي إلى عدم إمكانية تنظيم نظام التشفير بحيث تجري حماية مفتاح عن طريق مفتاح آخر كما نشير إلى ضرورة وجود مفتاح أعلى قمة هرم المفاتيح. يجري توليد وتوزيع هذا «المفتاح الرئيسي» في صورة مكونات منفصلة. ويجري امتلاك هذه المكونات بصورة منفصلة، وكذلك تُوضع بصورة منفصلة في جهاز التشفير. بداهةً، حتى يكون مفهوم استخدام المكونات ذا معنًى، يجب الحيلولة دون تمكن أي شخص من الحصول على المفتاح بجميع مكوناته في صورة واضحة.

ننتقل الآن إلى عرض الطريقة التي يجري بها بناء مكونات المفتاح بحيث لا تعطي أي معلومات عن المفتاح. هب أننا نرغب في وجود مكونين يمكن الجمع بينهما لبناء مفتاح K؛ يتمثَّل الأسلوب المباشر الساذج في استخدام النصف الأول من K كمكوِّن أول K_1 والنصف الثاني كمكون ثانٍ K_2. ومع ذلك سيصبح من الممكن اكتشاف المفتاح K بمعرفة المكون K_1 فقط من خلال تجريب جميع القيم الممكنة للمكون الثاني K_2. على سبيل المثال، إذا كان المفتاح K يتألف من 64 رقمًا ثنائيًّا، فستؤدي معرفة K_1 إلى اكتشاف المفتاح من خلال 2^{32} محاولة فقط، وهو عدد المحاولات اللازمة لاكتشاف K_2، وهو عدد لا يُذكر من المحاولات عند مقارنته بعدد المحاولات اللازمة لإجراء عملية بحث شاملة عن المفتاح K، والتي تبلغ 2^{64} محاولة. يتمثَّل حل آخر أفضل بكثير في توليد مكونين K_1 وK_2 لهما نفس حجم K؛ بحيث يكون المفتاح K هو نتاج إجراء عملية إكس أو آر للمكونين K_1 وK_2 ($K = K_1 \oplus K_2$). وبما أن K وK_2 لهما الحجم نفسه، لا تسفر معرفة المكون K_1 عن وسيلة أسرع لاكتشاف المفتاح K؛ إذ إن البحث عن K_2 ليس أسهل من البحث عن K.



بيئة نقطة إلى نقطة   بيئة المركز والطرف   بيئة متعدد إلى متعدد

أحد الأساليب الأكثر تعقيدًا هو تطبيق مفهوم «نظام الأنصبة السرية». في هذا السيناريو، يوجد عدد من القيم، يطلق عليه اسم الأنصبة، ويجري الحصول على المفتاح من خلال دمج بعض أو جميع الأنصبة. على سبيل المثال، يتمثل أحدُ الاحتمالات في وجود سبعةِ أنصبة وتصميمِ النظام بحيث تحدد أيُّ أربعةٍ من الأنصبة المفتاحَ بدقة، فيما لا تسفر معرفة أي ثلاثة أنصبة عن أي معلومات بشأن المفتاح. لا يثير هذا مسألة الأمن المرتبطة بالمسئولية المشتركة فحسب، بل يقلل أيضًا من إمكانية الاعتماد على توافر أفراد بأعينهم في حال ضرورة استرجاع المفتاح.

مثلما هو الحال مع الكثير من سمات التشفير، تعتبر عملية إدارة المفاتيح في أنظمة الاتصال أصعب بكثير من إدارة البيانات المخزنة. في حال ما إذا كان المستخدم يحمي

معلوماته الخاصة وحسب، فعلى الأرجح لن تكون هناك حاجة إلى توزيع المفاتيح. لكن إذا كانت هناك حاجة إلى إجراء اتصالات سرية، فغالبًا ما يتطلب الأمر توزيع المفاتيح. بالإضافة إلى ذلك، يعتمد حجم المشكلة المصاحبة على الأرجح على عدد الأجهزة الطرفية التي تحاول الاتصال على نحو آمن. ففي حالة وجود جهازين فقط، يُطلق على ذلك اسم بيئة «نقطة إلى نقطة». وإذا كان هناك أكثر من جهاز في عملية الاتصال، فسيعتمد حل مشكلة توزيع المفاتيح على نوع تطبيق الأعمال والبيئة التي تشكلها الأجهزة الطرفية. هناك حلَّان على طرفيْ نقيض؛ يتمثل الحل الأول في بيئة «المركز والطرف»، التي تتألف من جهاز مركزي وعدد من الأجهزة الطرفية الأخرى التي يمكنها الاتصال بالمركز على نحو آمن. ويتمثل الحل الثاني في بيئة «متعدد إلى متعدد»، وهي بيئة تتوفر عندما يتطلب كل جهاز توفير قناة اتصال آمنة بجميع الأجهزة الأخرى.

يختلف الوضع بالنسبة إلى أنظمة المفاتيح المعلنة. جانب كبير من هذه المناقشة ينطبق على المفاتيح السرية التي تحتاج إلى الاحتفاظ بها سرية كما هو الحال بالنسبة للمفاتيح المتناظرة. ومع ذلك يجري تخزين المفاتيح المعلنة وتوزيعها من خلال شهادات، كما أشرنا في الفصل السابع.

(٢-٣) تحديد المفتاح

تتمثل فكرة تحديد المفتاح في توفر أسلوب لدى طرفين للاتفاق على مفتاح يستخدمانه فيما بينهما. ويطلق على هذا الأسلوب اسم «بروتوكول الاتفاق على المفتاح»، ويعتبر بديلًا لعملية توزيع المفاتيح. بطبيعة الحال، من الأهمية بمكان توفر القدرة لدي الطرفين على التحقق من هوية كلٍّ منهما قبل الاتفاق على المفتاح. إن استخدام شهادات المفتاح المعلن تجعل هذا الأمر ممكنًا. يرجع الفضل في ابتكار البروتوكول الأكثر شهرةً واستخدامًا من هذا النوع إلى ديفي وهلمان. وفق «بروتوكول ديفي-هلمان»، يتبادل الطرفان مفاتيحهما المعلنة. وباستخدام قاعدة مزج جرى انتقاؤها بعناية، يدمج كل طرف مفتاحه السري مع مفتاح الطرف الآخر المعلن، وهو ما يمنحهما قيمة مشتركة تُشتق منها قيمة المفتاح.

تعتبر الحاجة إلى تحقق كل مستخدم منهما من هوية الآخر في غاية الأهمية. فبدونه، يتعرض البروتوكول إلى ما يطلق عليه اسم «اعتراض الطرف الدخيل». في مثل هذا النوع من الاعتراض، يعترض طرف دخيلٌ الاتصالاتِ بين الطرفين الأصليَّيْن، ثم ينتحل شخصية كلٍّ منهما عند اتصالهما أحدهما بالآخر. ينتج عن ذلك اعتقاد الطرفين أنهما اتفقا على

مفتاح، بينما اتفق كل طرف في حقيقة الأمر على مفتاح مع «الطرف الدخيل». تعد هذه الحالة إحدى الحالات التي تصبح فيها الشهادات الرقمية في غاية الأهمية.

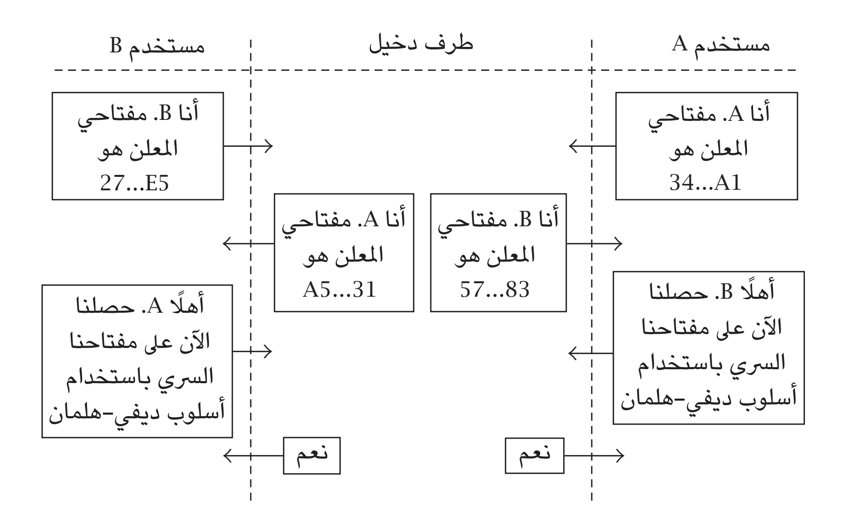
تتمثل الفكرة الأساسية في بروتوكول ديفي-هلمان في أنه على الرغم من قدرة الأطراف المعترضة على التلصص على عمليات اتصال تحديد المفتاح، لا تستطيع تلك الأطراف حساب المفتاح. يعتبر أسلوب التشفير الكمي أسلوبًا جديدًا مثيرًا لا يعتمد على قوة خوارزمية التشفير؛ حيث يستعين طرفا عملية الاتصال بخواص ميكانيكا الكم عند نقل المعلومات ولاكتشاف أي عملية اعتراض أثناء الاتصال. وتتضمن عمليةُ الاتفاق على مفتاحٍ ما إرسالَ المستخدم متتالية عشوائية من البيانات إلى مستخدم آخر. فإذا جرى اعتراض هذه المتتالية، يمكن اكتشاف عملية الاعتراض هذه، وتُجرى عملية الاتفاق على المفتاح من جديد، ثم يجري استخدام المتتالية التي لا يحدث اعتراض لها كأساس في تصميم المفتاح.

(٤-٢) استخدام المفاتيح

في كثير من الأنظمة، يجري تخصيص استخدام محدد لكل مفتاح بحيث لا يُستخدم كل مفتاح إلا للغرض الذي صُمم من أجله. يبدو أن هذا الشرط لا يكون مبررًا دائمًا. ومع ذلك كانت هناك دون شك حالات نتجت فيها مواطن ضعف في النظام جراء الاستخدامات المتعددة لمفتاح واحد. حاليًّا، يعد من قبيل الممارسات الجيدة الاستمرار في الفصل بين الاستخدامات.

رأينا أمثلة تبين أن مفهوم استخدام المفاتيح لغرض واحد يُعد فكرة جيدة. على سبيل المثال، ناقشنا من قبل استخدام المفاتيح لتشفير مفاتيح أخرى، وهو ما يختلف عن تشفير البيانات. ولفهم قيود الاستخدام عمليًّا، سنحتاج إلى الحديث من جديد عن مفهوم «نموذج أمن مقاومة التلاعب». إذا تلقى أحد المستخدمين نصًّا مشفرًا، إذن ففي ظل النص المشفر والمفتاح المناسب كمدخلات لنموذجِ أمنِ مقاومةِ التلاعبِ، سيتوقع المستخدم أن يعطي نموذجُ أمن مقاومة التلاعب البياناتِ المطلوبة كمخرج. غير أنه إذا تلقى المستخدم مفتاحًا مشفَّرًا، فلن يحتاج إلى الحصول على المفتاح في صورة واضحة كمخرج لنموذج أمن مقاومة التلاعب، بل سيرغب في فك شفرة المفتاح واستخدامه في النموذج. ولكنْ كلٌّ مِن النص المشفر والمفتاح عبارة عن سلسلة أرقام ثنائية لا تستطيع

خوارزمية التشفير التمييز بينهما. بناءً عليه، يجب أن يرتبط مفهوم استخدام المفتاح بوظيفة نموذج أمن مقاومة التلاعب وليس بالخوارزمية المستخدمة.



طرف دخيل.

حتى يصبح لكل مفتاح استخدام محدد، يجب تخصيص علامة تمييز لكل مفتاح تحدد الغرض منه. على سبيل المثال، قد تحدد العلامة أيًّا من الوظائف الآتية: «مفتاح تشفير بيانات»، و«مفتاح تشفير مفاتيح»، و«مفتاح توليد شفرة اعتماد رسائل»، و«مفتاح تحقق من شفرة اعتماد رسائل». بطبيعة الحال، يعتمد شكل هذه العلامة على نموذج أمن مقاومة التلاعب وعلى بيئة النظام. في حالة الخوارزمية غير المتناظرة، ربما يحتاج المستخدمون زوجين من المفاتيح المعلنة والسرية؛ زوجًا لاستخدامه في عملية التشفير وزوجًا آخر لاستخدامه في التوقيعات الرقمية.

بمجرد الاتفاق على علامات التمييز، يجب توفر أسلوب لربط العلامة بالمفتاح بحيث لا يستطيع الخصوم تغيير العلامة؛ ومن ثَمَّ يسيئون استخدام المفتاح. تتمثل إحدى هذه الطرق في جعل جميع النسخ المشفرة من المفتاح تعتمد على المفتاح الأعلى في نموذج أمن مقاومة التلاعب وعلامة تمييز المفتاح، وهو ما يضمن عدم إمكانية «إزالة» العلامة

إلا في نموذج أمن مقاومة التلاعب. بمجرد ربط علامات التمييز بالمفاتيح، يجب توفر آلية لضمان عدم إساءة استخدام المفاتيح. يعتبر تصميم وتشكيل نموذج أمن مقاومة التلاعب من الأهمية البالغة بمكان في تنفيذ هذه الآلية.

(٢-٥) تغيير المفاتيح

في جميع أنظمة التشفير، يجب توفر القدرة على تغيير المفاتيح. ثمة أسباب عديدة وراء ذلك، وقد تحدث عملية التغيير وفق تحديثات منتظمة تخضع لجدول زمني أو كاستجابة لاشتباه في عملية اعتراض. في حال الشك في اعتراض المفتاح، يجب تغييره على الفور. تُجري العديد من المؤسسات عملية اختبار دورية لتغيير المفاتيح؛ بحيث تصبح مستعدة لأي حالات طوارئ، ويمتلك طاقم العاملين فيها الخبرة العملية المناسبة.

تتغير المفاتيح بانتظام للحد من سُبل انكشافها والتقليل من أهميتها حال الكشف عنها عن طريق طرف معترض. لا شك في أن قيمة عملية اعتراض ناجحة تحدد الوقت والجهد اللذين من المرجح أن يستثمرهما الطرف المعترض في عملية الاعتراض. توجد أنظمة إلكترونية لنقل الأموال عند نقطة البيع، يتغير المفتاح فيها بعد كل معاملة. لا يُحتمل في مثل هذه الأنظمة أن يَستثمر الطرف المعترض موارد ضخمة لتنفيذ عملية اعتراض لن تسفر إلا عن انكشاف مفتاح واحد ومعاملة واحدة.

بينما لا توجد قواعد واضحة حول معدلات تغيير المفاتيح، فإنه من الواضح أن كل مفتاح يجب تغييره قبل فترة طويلة من تعيينه باستخدام عملية البحث الشامل عن المفتاح. هناك عامل آخر يتمثَّل في المخاطر المتصورة المتمثلة في تحقيق التوازن بين اكتشاف المفتاح والمخاطر المصاحبة لتغييره.

(٢-٦) تدمير المفاتيح

يجب تدمير المفاتيح بطريقة آمنة متى انتهت الحاجة إليها. بناءً عليه، لا يعتبر مجرد محو الملف الذي يحتوي على قيمة المفتاح كافيًا. يُوصى في كثير من الأحيان بوضع بيان تفصيلي بطريقة تنفيذ عملية التدمير. على سبيل المثال، يَنُص أحد معايير معهد المعايير القومي الأمريكي على الآتي: «يجب تدمير الوسائط الورقية التي تحتوي على المفاتيح عن طريق التمزيق، أو الفرم، أو الحرق، أو الإذابة. يجب تدمير مواد المفاتيح المخزنة على

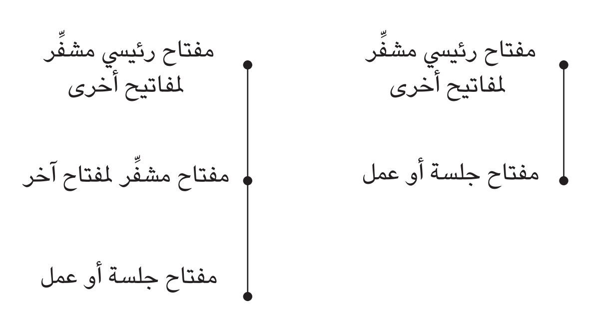
أي وسائط أخرى بحيث لا يمكن بأي حال من الأحوال استرجاعها من خلال أي وسائل مادية أو إلكترونية.» يعني ذلك على وجه الخصوص أن جميع المفاتيح المخزنة بوسائل إلكترونية يجب التخلص منها بتسجيل بيانات مكانها دون الاكتفاء بمحوها؛ بحيث لا تخلِّف أثرًا أو أي معلومات أخرى قد تفيد الأطراف المعترضة. تعتبر هذه المسألة في غاية الأهمية في تطبيقات البرامج؛ إذ قد يجري استخدام الذاكرة المستخدمة في تخزين المفاتيح في أغراض أخرى لاحقًا.

(٣) التسلسلات الهرمية للمفاتيح

مثلما أشرنا، تعتبر العمليات اليدوية مكلفة فضلًا عن استغراقها وقتًا طويلًا؛ لذا يُفضل استخدامها في أضيق الحدود. بناءً عليه، في حالة إدارة المفاتيح، متى كان ذلك ممكنًا، يُفضَّل توزيع المفاتيح إلكترونيًّا عن توزيعها يدويًّا. لكنه إذا جرى توزيع مفتاح إلكترونيًّا، فسيحتاج المفتاح حماية من انكشافه أثناء عملية انتقاله. تتمثل الطريقة المفضلة لتحقيق ذلك في تشفير المفتاح عن طريق مفتاح آخر. مثلما أشرنا سابقًا، يقودنا هذا إلى مفهوم المفاتيح الهرمية؛ حيث لا يوجد أي مفتاح يحمي المفتاح الرئيسي. بناءً عليه، يجب توزيع المفتاح الرئيسي يدويًّا، سواءٌ من خلال جهاز مقاومة تلاعب أو من خلال تقسيمه إلى مكونات منفصلة.

يتمثل الشكل الأبسط للسلسلة الهرمية للمفتاح في سلسلة تتألف من طبقتين. يعتبر المفتاح الرئيسي مفتاح تشفير مفاتيح، ويُستخدم حصريًّا في حماية المفاتيح في المستويات الأدنى. يُطلق على مفاتيح المستويات الأدنى «مفاتيح جلسات» أو «مفاتيح عمل». تختلف وظيفة هذه المفاتيح حسب الغرض من تطبيقها. على سبيل المثال، قد تُستخدم هذه المفاتيح في تشفير البيانات لتحقيق السرية أو لحساب كود توثيق الرسائل للتحقق من سلامة البيانات. يمكن تعريف الجلسة بعدة طرق، ربما من خلال فترة زمنية أو عدد الاستخدامات. عند ظهور الحاجة إلى تغيير مفتاح الجلسة، يجري توزيع المفتاح الجديد في ظل حماية المفتاح الرئيسي. ومع ذلك، إذا استدعت الضرورة تغيير المفتاح الرئيسي، يجب إجراء هذه العملية يدويًّا. غالبًا ما تكون عمليات تغيير المفاتيح يدويًّا غير عملية؛ ومن ثَمَّ تتضمن العديد من الأنظمة تسلسلات هرمية تتألف من ثلاث طبقات، مع وجود طبقة إضافية بين المفتاح الرئيسي ومفتاح الجلسة. تُستخدم المفاتيح في هذه

الطبقة الإضافية في تشفير مفاتيح أخرى، وينحصر دورها في حماية مفاتيح الجلسات. في المقابل، يمكن توزيع مفاتيح التشفير هذه في ظل حماية المفتاح الرئيسي. تسمح هذه الطبقة الإضافية بتغيير مفاتيح تشفير المفاتيح إلكترونيًّا كما تُقلل كثيرًا من احتمال اللجوء إلى تغيير المفاتيح يدويًّا. يُبيِّن الشكل السابق هذين الخيارين؛ حيث «يحمي» كلُّ مفتاح المفتاحَ الذي يقع في المستوى الأدنى منه.



تراتبيات مفاتيح بسيطة.

خلال مناقشتنا لعملية إدارة المفاتيح، افترضنا أن مفاتيح العمل تناظرية، ومع ذلك لا يوجد تبرير لأنْ تكون الخوارزمية المستخدمة في تشفير مفاتيح العمل هي نفسها الخوارزمية المُستخدمة لحماية البيانات. وعلى وجه الخصوص، لا يَمنع كونُ مفاتيح العمل تناظريةً استخدامَ نظام تشفير المفاتيح المعلنة في تصميم مفاتيح المستويات العليا. في حقيقة الأمر، توجد أنظمة «هجينة» كثيرة تُستخدم فيها الخوارزميات غير المتناظرة في توزيع المفاتيح في أنظمة الخوارزميات المتناظرة.

(٤) إدارة المفاتيح في الشبكات

إذا أراد طرفان تبادل رسائل مشفرة، يوجد عدد من الخيارات أمامهما لإدارة المفاتيح، وهو ما يعتمد على بيئة الاتصال ومستوى الأمن المطلوب. يمكن أن يلتقي المستخدمان وجهًا لوجه لتبادل قيم المفاتيح مباشرةً. إذا اتفق المستخدمان على استخدام أحد برامج التشفير، فقد ييسر هذا البرنامج من إجراءات الاتفاق على المفتاح عن طريق استخدام

برتوكول مثل بروتوكول ديفي–هلمان. ومع ذلك ربما تكون تكلفة أحد برامج التشفير مرتفعة أو معقدة للغاية. على سبيل المثال، هناك برامج توفر خوارزمية تشفير كما تقدم نصائح إلى المستخدم حول بناء المفتاح في صورة رموز تتألف من أحرف هجائية وأعداد. يُشار على الطرف المرسل بعدئذٍ بتمرير قيمة المفتاح إلى الطرف المستقبل عن طريق مكالمة هاتفية. لا شك في وجود تداعيات أمنية لذلك، لكن وسيلة تمرير المفتاح على هذا النحو تكون مقبولة في معظم الاتصالات الشخصية. ومع ذلك لا يرغب معظم الناس في إزعاج أنفسهم بإجراء مكالمة هاتفية لإرسال رسالة بريد إلكتروني سرية.

إذا كان مستوى الأمن المطلوب مرتفعًا، فسيتضمن الاتفاق المبدئي على الأرجح إجراء عملية يدوية بصورة أو بأخرى. بما أن العمليات اليدوية تنحو إلى أن تكون بطيئة ومكلفة، يحاول المستخدمون على الأرجح ضمان إجراء جميع الاتفاقات المستقبلية على المفاتيح إلكترونيًّا. في حال كانت الشبكة صغيرة بما يكفي، يتمثل أحد خيارات توزيع المفاتيح في تصميم مفتاح مشترك بين كل زوج من الأجهزة. ومع ذلك قد تستغرق هذه العملية وقتًا طويلًا، فضلًا عن تكلفتها. وفي حال كانت الشبكة كبيرة، فهناك احتمال لأنْ تصبح عملية إدارة المفاتيح عبئًا لا يمكن تحمُّله. للتغلب على هذه المشكلة، لدى العديد من الشبكات مراكز محل ثقة تتضمن الأدوار التي تؤديها تيسير عملية تصميم مفاتيح بين أزواج المستخدمين في الشبكة.

يتضمن أحد السيناريوهات التقليدية أن يقوم كل مستخدم بتحديد مفتاح مشترك مع مركز محل للثقة. وعلى الرغم من أن ذلك يستغرق وقتًا طويلًا فضلًا عن تكلفته، يتعين إجراء هذه العملية مرة واحدة فقط. فإذا أراد مستخدمان الاتصال سرًّا، فإنهما يعودان إلى المركز محل الثقة لتصميم مفتاح مشترك عن طريق استخدام مفاتيح سرية مشتركة متوفرة لدى المركز وكلا المستخدمين. تعتمد الحلول التي نقترحها هنا على معايير معهد المعايير القومي الأمريكي والمنظمة الدولية للمعايير.

(٥) استخدام مركز إدارة محل ثقة

يتعلق السيناريو الذي نناقشه بشبكة كبيرة الحجم تتطلب فيها كل نقطة اتصال قناة مشفَّرة آمنة للاتصال بنقطة اتصال أخرى. يحتِّم حجم الشبكة استخدام مركز محل ثقة لتيسير تصميم مفتاح سري آمن بين أي نقطتَيِ اتصال. نفترض أن كل نقطة

اتصال أنشأت قناة اتصال آمنة ودائمة مع المركز. وهكذا، قد تتطلب أي نقطتَيِ اتصال اللجوء إلى المركز محل الثقة لتصميم مفتاح سريٍّ مشترك بينهما.

على الرغم من استخدام نقطتَي الاتصال خوارزميةً متناظرة لتحقيق الاتصال الآمن بينهما، قد تكون الخوارزمية المستخدمة في تحقيق الاتصال الآمن بين المركز وأي نقطة اتصال متناظرة أو غير متناظرة. إذا جرى استخدام خوارزمية متناظرة في النظام كله، فسيكون المركز محل الثقة «مركز توزيع المفاتيح» أو «مركز ترجمة المفاتيح». في حالة استخدام خوارزمية غير متناظرة، فسيكون المركز محل الثقة «مركز اعتماد المفاتيح». وسنتناول كلتا الحالتين على التوالي.

هَبْ أن خوارزمية متناظرة جرى استخدامها عبر النظام كله؛ إذا رغبت نقطة الاتصال A في إجراء اتصالات آمنة مع نقطة الاتصال B، تتقدم A بطلب إلى مركز الاتصال محل الثقة لتصميم مفتاح سري مشترك بين A وB. باستخدام مركز توزيع المفاتيح، تطلب نقطة الاتصال A من مركز توزيع المفاتيح توفير المفتاح، بينما عند استخدام مركز ترجمة المفاتيح، تولِّد نقطة الاتصال A المفتاح ثم تقدِّم طلبًا إلى مركز ترجمة المفاتيح لِتُمكنها من توزيع المفتاح بأمان إلى نقطة الاتصال B. في كلتا الحالتين، يمكن استخدام المفاتيح المشتركة بين A وB والمركز محل الثقة، كمفاتيح لتشفير مفاتيح أخرى بغرض حماية جميع الاتصالات بين كلٍّ من نقطتَي الاتصال والمركز. إذا أطلقنا على المفتاح الجديد اسم KAB، إذن فمتى انتقل KAB فستجري حمايته من خلال أيٍّ من المفاتيح المشتركة بين نقطتَي الاتصال والمركز. بناءً عليه، تعتمد نقطتا الاتصال A وB على سرية المفاتيح المشتركة بينهما وبين المركز؛ لثقتهما في أن نقاط الاتصال الوحيدة التي تعرف المفتاح KAB هي A وB فقط.

هب الآن أننا استخدمنا خوارزمية غير متناظرة بين المركز محل الثقة ونقطتَي الاتصال؛ نفترض رغبة نقطتَي الاتصال في إجراء اتصالات بينهما وفي توفير أزواج من المفاتيح المعلنة والسرية، نفترض أيضًا أن مركز اعتماد المفاتيح يعرف قيم هذه المفاتيح المعلنة كما يضمن صحة قيم المفاتيح هذه لكلٍّ مِن نقطتَي الاتصال A وB. تتمثل أبسط الطرق لتحقيق ذلك في أن يلعب مركز اعتماد المفاتيح دور جهة الاعتماد، وأن يصدر شهادات تربط بين نقطتَي الاتصال A وB والمفاتيح المعلنة لكلٍّ منهما. هب أن نقطة الاتصال A تولِّد المفتاح المتناظر KAB لإجراء اتصال آمن مع نقطة الاتصال B؛ تشفِّر نقطة الاتصال A المفتاح المتناظر KAB باستخدام المفتاح المعلن لنقطة الاتصال B، ثم

توقِّع على النتيجة باستخدام المفتاح السري لنقطة الاتصال A. يؤدي تشفير المفتاح KAB باستخدام المفتاح المعلن لنقطة الاتصال B إلى ثقة نقطة الاتصال A في أن المفتاح المتناظر KAB معروف لنقطة الاتصال B فقط. بالإضافة إلى ذلك، يؤدي توقيع المفتاح KAB باستخدام المفتاح السري لنقطة الاتصال A إلى ثقة نقطة الاتصال B في أن المفتاح المتناظر KAB مصدره نقطة الاتصال A. بناءً عليه، تثق نقطتا الاتصال A وB في أنهما وحدهما تعرفان المفتاح المتناظر KAB.

يمكن استخدام المفتاح المتناظر المشترك بين A وB كمفتاح لتشفير مفاتيح أخرى أو كمفتاح عمل. وإذا كان KAB مفتاح تشفير مفتاح آخر، فلن تحتاج أبدًا نقطتا الاتصال إلى استخدام مركز الاتصال محل الثقة مجددًا لتصميم مفاتيح عمل. بالإضافة إلى ذلك، لا يستطيع مركز اعتماد المفاتيح حساب المفتاح المتناظر KAB في حال توليد كلٍّ مِن A وB لأزواج مفاتيحهما المعلنة والسرية. ومع ذلك في حال استخدام مركز توزيع مفاتيح أو مركز ترجمة مفاتيح، يجب ظهور المفتاح المتناظر KAB في صورة واضحة في المركز محل الثقة.

(٦) استرجاع المفاتيح والمفاتيح الاحتياطية

سيحتاج كلُّ مَن يريد الحصول على النص الأصلي المقابل لأحد النصوص المشفرة تحقق واحدة على الأقل من الحالات الآتية:

(١) الحصول على النص الأصلي.
(٢) معرفة خوارزمية فك التشفير والحصول على مفتاح فك التشفير.
(٣) معرفة خوارزمية فك التشفير والقدرة على كسرها.
(٤) تحديد موضع النص الأصلي في بنية النظام.
(٥) معرفة خوارزمية فك التشفير وتحديد موضع مفتاح فك التشفير في بنية النظام.
(٦) القدرة على استنباط الخوارزمية وكسرها.

في حال تحققت الحالة ١، لن يحتاج الطرف المعترض إلى إجراء أي عملية فك تشفير، بينما لو تحققت الحالة ٢ سيحصل الطرف المعترض على نفس المعلومات التي يتلقاها الطرف المستقبل الأصلي. يتمثل الهدف من استخدام التشفير القوي في منع عمليات الاعتراض مثلما هو الحال في الحالة ٣. في المقابل، لا يصبح استخدام التشفير

القوي ذا قيمة في الحالتين ٤ و٥. في حال تحقق الحالة ٤، يمكن أن يتغاضى الطرف المعترض عن إجراء أي عملية تشفير، بينما تعني الحالة ٥ أن الطرف المعترض يمتلك المعرفة نفسها المتوفرة لدى المستقبل الأصلي دون الحاجة إلى كسر الخوارزمية. بناءً عليه، من الأهمية بمكان أن يجري تأمين المفاتيح خلال دورة حياتها الكاملة. ناقشنا عملية إدارة المفاتيح بالتفصيل، لكننا لم نذكر بعدُ موضوعَ المفاتيح الاحتياطية المهمَّ. من الأهمية بمكان إدراك أن المعلومات الحيوية قد تُفقَد إلى الأبد في حال تشفيرِها باستخدام خوارزمية قوية ثم فقدانِ أو تلف المفتاح بعد ذلك. بناءً عليه، من الأهمية بمكان تَوفر نسخ احتياطية للمفتاح يجري تخزينها بأمان لدى صاحبها أو لدى طرف ثالث محل ثقة. نفترض هنا تحقق أسوأ السيناريوهات المذكورة؛ لذا لن نناقش الحالة ٦.

عند حديثنا عن التشفير، تبنَّينا الموقف القائل بأن التشفير أداة يستخدمها الأفراد أو الشركات لحماية الاتصالات السرية أو المعلومات المخزنة، كما توفر أيضًا الحماية للمجرمين والإرهابيين من سلطات إنفاذ القانون والهيئات الحكومية الأخرى. رأت سلطات إنفاذ القانون لسنوات عديدة أن اعتراض الاتصالات أمر مهم جدًّا في محاربة الجريمة. واعترافًا بذلك، توجد لدى الكثير من الدول تشريعات منذ فترة طويلة تسمح، في ظل ظروف محددة، بالاعتراض القانوني لبعض الاتصالات، مثل المكالمات الهاتفية. تدفع أجهزة الاستخبارات بحجج مشابهة في سعيها لمحاربة الإرهاب والمخاطر الأخرى التي تهدد الأمن القومي. وتباينت طرق استجابة الدول لهذه المشكلات؛ فقد حاولت بعض الحكومات التمسك برقابتها الصارمة لجميع استخدامات التشفير، بينما قصرت دول أخرى، بما فيها الولايات المتحدة والمملكة المتحدة، سيطرتها على تصدير أجهزة التشفير. ومع ذلك أدت التطورات الأخيرة، خاصةً الانتشار السريع لاستخدام برامج خوارزميات التشفير، إلى أن تُعيد معظم الحكومات النظر في سياساتها حيال استخدام التشفير.

ثمة تعارض واضح في المصالح بين الأفراد والمؤسسات، الذين يريدون حماية بياناتهم السرية، وبين هيئات إنفاذ القانون، التي تشدد على حاجتها إلى قراءة بعض المراسلات التي تعترضها لمحاربة الجريمة وحماية الأمن القومي. ترغب الشركات في إجراء عمليات تشفير قوية بما يكفي لمنع عصابات الجريمة المنظمة مِن فكها، في حين تريد الحكومات الاطلاع، في ظل ظروف محددة، على محتويات أي عملية اتصال.

يتعلق قانون تنظيم سلطات التحقيق لعام ٢٠٠٠ في المملكة المتحدة بعملية اعتراض الاتصالات. ولا عجب أن القسم الخاص بعملية الاعتراض المشروع للاتصالات في هذا

القانون كان مثارًا لجدل ونقاش كبيرين. يدور جزء من هذا الخلاف حول الاشتراط القائل بأن هيئات إنفاذ القانون قد تطلُب، وفق ظروف محددة، مفتاحَ التشفير اللازم لفك شفرة نص مشفَّر جرى اعتراضه، أو أن تحصل على النص الأصلي المقابل في صورة واضحة.

يتعلق جانب كبير من النقاش، تأكيدًا، بالجانب الأخلاقي المتمثل فيما إذا كان من حق هيئات إنفاذ القانون طلب المفاتيح تحت أي ظرف. ويعتبر هذا الجدل مثالًا حديثًا على النقاش القديم القائم حول تحقيق التوازن بين حريات الأفراد ومتطلبات الدولة. وفي حين لا نعتزم اتخاذ أي موقف في هذا الكتاب حيال هذا الموضوع، نلفت الانتباه إلى أنه، من الناحية الفنية، قد يرى أي مستخدم يقبل تفويض هيئات إنفاذ القانون سلطة قراءة البيانات المشفَّرة وفق ظروف محددة أن في صالحه تحقُّق الحالتين ١ أو ٢ فقط المذكورتين ضمن الحالات الست السابقة. وإذا تحققت أيٌّ من الحالات ٣–٦ من جانب هيئات إنفاذ القانون، فإن هذه الحالات أيضًا يمكن أن تتحقق على الأرجح بالنسبة إلى طرف مناوئ تتوفر له موارد كافية لتنفيذ عمليات الاعتراض.

استخدام التشفير من قبل الأفراد لتوفير السرية في وسائل الاتصال مثل البريد الإلكتروني ليس منتشرًا على نطاق واسع مثلما كان متوقعًا. لا يرجع ذلك، بالتأكيد، إلى نقص الخوارزميات المتاحة. على العكس تمامًا، تتوفر خيارات لا حصر لها من الخوارزميات العلنية المتاحة للمستخدمين الراغبين في استخدام التشفير، وهي الخوارزميات التي كانت ولا تزال تخضع إلى التدقيق الأكاديمي المفتوح وتبدو قوية جدًّا. الأرجح أن السبب الرئيسي هو غياب خوارزميات سهلة الاستخدام. لا يهتم معظم الأفراد بعملية الأمن بالقدر الذي يكفي لأنْ يكونوا على استعداد لبذل المزيد من الجهد لتحقيقه. عند إرسال رسالة بريد إلكتروني، لا يرغب المستخدم عادةً إلا في ضغط زر «أرسلْ». في المقابل، يثير طلب استخدام التشفير عادةً سلسلة من الأسئلة من الكمبيوتر الذي يتوقع الحصول على إجابات أو اتخاذ إجراءات من قِبل المستخدم. لا يعبأ كثير من المستخدمين بذلك. جانب كبير من الإزعاج المصاحب لعملية التشفير بالنسبة إلى المستخدمين يتمثل في إدارة المفاتيح. لسوء الحظ، وكما أكدنا مرارًا، تعتبر الإدارة الجيدة للمفاتيح مسألة في غاية الأهمية لتحقيق الأمن الشامل للنظام.

الفصل التاسع

التشفير في الحياة اليومية

(١) مقدمة

شددنا مرارًا عبر صفحات الكتاب على أهمية التشفير في الحياة الحديثة وعرضنا نماذج من الحياة الواقعية لبيان بعض الموضوعات المهمة. يشتمل هذا الفصل على بعض الموضوعات المتفرقة التي يُيسِّر فيها استخدام التشفير توفير خدمة آمنة. وفي حين تمثِّل معظم هذه الموضوعات سيناريوهات لمواقف يواجهها رجل الشارع العادي بصورة شبه يومية، فإنه لا يعطي قدرًا كافيًا من الاهتمام للمخاطر الأمنية التي تنطوي عليها مثل هذه المواقف أو للدور الذي تلعبه عملية التشفير. نعرض تفاصيل الاستخدام في كل حالة من الحالات، ونناقش الموضوعات الأمنية ذات الصلة، ونبين طريقة استخدام التشفير.

(٢) عملية سحب نقدي من ماكينة صرَّاف آلي

عندما يجري أحد الأشخاص عملية سحب نقدي من ماكينة صرَّاف آلي، يجب عليه امتلاك بطاقة بلاستيكية تحتوي على شريط ممغنط وإدخال رقم التعريف الشخصي المرتبط بها. يُدخل العميل البطاقة في الفتحة المخصصة لها في الماكينة ثم يُدخل رقم التعريف الشخصي، ثم يُدخل القيمة النقدية التي يرغب في سحبها. عادةً عند إجراء معاملة، يحتاج النظام إلى التأكد من أن رقم التعريف الشخصي هو الرقم الصحيح للبطاقة التي جرى إدخالها، وفي حال إجراء المعاملة على الإنترنت، سيحتاج النظام إلى التأكد من جواز سحب العميل للقيمة النقدية المطلوبة. تجري عملية التحقق هذه على الأرجح عبر الكمبيوتر المركزي للمصرف؛ ومن ثَمَّ يجب توفر وسيلة اتصال في اتجاهين بين الماكينة والكمبيوتر المضيف. تُرسل الماكينة بيانات البطاقة ورقم التعريف الشخصي

إلى الكمبيوتر المضيف، ثم تأتي الإجابة من الكمبيوتر المضيف بالتصريح بإجراء المعاملة أو رفضها. بداهةً، تحتاج عمليات الاتصال هذه إلى حماية.

على الرغم من عدم سرية قيمة النقد المسحوبة، من الأهمية بمكان تَطابُق القيمة المسحوبة من الماكينة مع القيمة المخصومة من الحساب المصرفي. بناءً عليه، تحتاج الرسالة التي تظهر على شاشة الماكينة إلى أحد أشكال حماية النزاهة. بالإضافة إلى ذلك، ينتاب المصارف القلق، وهو أمر مفهوم، حيال إمكانية إصدار النقد أكثر من مرة من ماكينة الصرَّاف الآلي من خلال نفس الرسالة. بناءً عليه، هناك شرط آخر يتمثل في تضمين أرقام متسلسلة على رسائل سحب النقد لمنع تكرار عمليات السحب من خلال رسالة معاملة السحب نفسها.

تنبه جميع المصارف عملاءها إلى الحفاظ على سرية أرقام تعريفهم الشخصية؛ حيث إن كلَّ مَن يعرف رقم التعريف الشخصي الصحيح سيستطيع استخدام البطاقة المسروقة أو المفقودة. بداهةً، يجب على المصارف ضمان عدم اعتراض أرقام التعريف الشخصية في نظمهم المصرفية؛ ومن ثَمَّ يجري تشفير أرقام التعريف الشخصية خلال نقلها وفي قاعدة البيانات المستخدمة في التحقق من صحة الأرقام. الخوارزمية المستخدمة في هذه العملية هي معيار تشفير البيانات وفق نمط كتاب الشفرات الإلكتروني. بما أن نظام معيار تشفير البيانات يشفِّر كتلًا تتألف كلٌّ مِنها من 64 رقمًا ثنائيًّا، وحيث إن أرقام التعريف الشخصية تتألف عادةً من أربعة أعداد فقط؛ يجب إجراء عملية إضافة أرقام ثنائية للكتلة التي تشتمل على رقم التعريف الشخصي قبل تشفيرها. إذا كان نتاج عملية الإضافة متطابقًا بالنسبة لجميع العملاء، حتى بالرغم من عدم امتلاكهم المفتاحَ الصحيح، فسيتمكن كلُّ مَن يستطيع التوصل إلى المجموعات المشفرة لأرقام التعريف الشخصية من تحديد هوية العملاء الذين يشتركون في رقم التعريف الشخصي نفسه. يمكن التخلص من وجه القصور المحتمل هذا من خلال استخدام أسلوب إضافة أرقام ثنائية للكتل، تعتمد على تفاصيل بطاقة العميل.

يَمنع استخدام عملية التشفير على هذا النحو انكشاف رقم التعريف الشخصي للمتلصصين الذين يعترضون الاتصالات بين ماكينة الصراف الآلي والكمبيوتر المضيف، كما يمنع ذلك أيضًا قراءة أرقام التعريف الشخصية من قِبل أفراد مفوضين بالاطلاع على قاعدة بيانات المصرف. ومع ذلك، مثلما ذكرنا سابقًا، لا تمنع عملية التشفير أحد المحتالين من تخمين رقم التعريف الشخصي لأحد العملاء. يستطيع كلُّ مَن يعثر على

البطاقة البلاستيكية أو يسرقها إدخالها في ماكينة الصراف الآلي ومحاولة إدخال رقم يعتمد في صحته على الحظ. وبما أن هناك ما لا يزيد عن 10 آلاف رقم تعريف شخصي يتألف من أربعة أرقام، فلا تعتبر فرص نجاح عملية تخمين الرقم الصحيح ضئيلة. اعترافًا بذلك، تسمح معظم ماكينات الصراف الآلي بإجراء ثلاث محاولات فقط لإدخال رقم التعريف الشخصي قبل «احتجاز» البطاقة بالماكينة. يعتبر هذا حلًّا وسطًا معقولًا يحقق التوازن بين المخاطر الأمنية التي تسمح للمحتالين بإجراء العديد من المحاولات وبين مخاطر ارتكاب حاملي البطاقات الأصليين أخطاءً عند إدخال أرقام تعريفهم الشخصية. مثلما أشرنا، لا يوفر استخدام التشفير الحماية ضد تخمين رقم التعريف الشخصي.

تستخدم بعض شبكات الصراف الآلي حاليًّا بطاقات ذكية تسمح باستخدام نظام تشفير المفاتيح المعلنة. تشتمل بطاقة المستخدم، إذن، على مفتاحه السري وشهادة، توقعها جهة إصدار البطاقة، لتأكيد قيمة مفتاحه المعلن. تتحقق ماكينة الصراف الآلي من البطاقة من خلال توجيه سؤال إلى المستخدم يتوجَّب عليه إجابته. مثلما هو الحال في جميع الأنظمة التي تعتمد على الشهادات، من الضرورة بمكان أن تتوفر نسخة صحيحة في ماكينة الصراف الآلي من المفتاح المعلن لجهة إصدار البطاقة بغرض ضمان صحة الشهادة. في بعض الأنظمة، يجري تحقيق ذلك من خلال تضمين قيمة المفتاح المعلن في ماكينات الصراف الآلي.

(٣) التليفزيون المدفوع

كلُّ مَن يشترك في أحد أنظمة التليفزيون المدفوع يتوقع مشاهدة البرامج التي دفع مقابل مشاهدتها، كما يتوقع أيضًا عدم إتاحة هذه البرامج لمن لم يدفعوا مقابل مشاهدتها. تعتبر أنظمة التليفزيون المدفوع أحد أمثلة شبكات البث التي يتم فيها التحكم في عملية الوصول إلى محتوياتها. في شبكات كهذه، يَجري بث المعلومات — في هذه الحالة البرامج التليفزيونية — على نطاق واسع، لكن لا يستطيع فَهْمَ هذه المعلومات سوى مجموعة محددة ممن يتلقَّون الإشارة. تتمثل إحدى الطرق الشائعة لتحقيق هذا الهدف في تشفير إشارة البث باستخدام مفتاح يجري توفيره فقط إلى المتلقين المقصودين للمعلومات. هناك طرق عديدة لتصميم وإدارة هذه الأنظمة.

في الأنظمة المعتادة للتليفزيون المدفوع، يجري تشفير كل برنامج من خلال رقم خاص به قبل عملية البث. وكلٌّ مَن يدفع لمشاهدة برنامج محدد، يدفع في الأساس لمعرفة المفتاح. بداهةً، يؤدي ذلك إلى بروز مشكلة إدارة المفاتيح التي تتمثل في القدرة على توصيل المفاتيح للمشاهدين المقصودين. يتمثَّل أحد الحلول الشائعة لتلك المشكلة في إصدار بطاقة ذكية لكل مشترك في الشبكة تحتوي على الرقم الخاص للمشترك باستخدام خوارزمية تشفير غير متناظرة. يجري بعد ذلك إدخال البطاقة الذكية في جهاز قراءة إما يمثل جزءًا من التليفزيون أو توفره شبكة التشغيل. عندما يدفع أحد المشتركين نظير مشاهدة أحد البرامج، يَجري نقلُ المفتاح المتناظر المستخدم في تشفير البرنامج مشفرًا مع المفتاح المعلن للمشترك. بناءً عليه، باستخدام مصطلحات الفصل الثامن، يَستخدم هذا النوع من الأنظمة مفتاحًا هرميًّا ذا مستويين من المفاتيح يتضمن استخدام مزيج من الخوارزميات المتناظرة وغير المتناظرة.

(٤) خصوصية آمنة تمامًا

جرى تطوير برنامج «خصوصية آمنة تمامًا» في صورته الأصلية من قِبل فيل زيمرمان في أواخر ثمانينيات القرن العشرين. كان الهدف من البرنامج هو أن يكون بمنزلة منتَج سهل الاستخدام لإجراء عمليات التشفير على أجهزة الكمبيوتر الشخصية باستخدام التشفير المتناظر وغير المتناظر. ويجري استخدام إصدارات عديدة منه حاليًّا. نناقش فيما يلي المفهوم العام دون التركيز على أيٍّ إصدار محدد أو تطبيقات البرنامج.

يستخدم برنامج «خصوصية آمنة تمامًا» مفتاحًا هرميًّا ذا مستويين يجري فيه استخدام مفاتيح الجلسات المتناظرة في حماية البيانات، فيما يجري استخدام المفاتيح غير المتناظرة في كلٍّ مِن إصدار التوقيعات وحماية مفاتيح الجلسات المتناظرة. يستخدم برنامج «خصوصية آمنة تمامًا» في كثير من التطبيقات، ويشمل ذلك حماية رسائل البريد الإلكتروني وتخزين الملفات بصورة آمنة. أدَّى نشر البرنامج على لوحة إعلانات عامة في عام ١٩٩١ إلى نشوب نزاع بين فيل زيمرمان وكلٍّ مِن الحكومة الأمريكية (لتصدير نظام تشفير بصورة غير قانونية) وعدد من حاملي براءات الاختراع. جَرَتْ تسوية هذه النزاعات في عام ١٩٩٧. حاليًّا، يتوفر برنامج «خصوصية آمنة تمامًا» كبرنامج مجاني وهو جزء من برامج الكثير من أجهزة الكمبيوتر الجديدة.

مثلما ذكرنا، تتمثل إحدى المشكلات الكبرى في استخدام نظام التشفير غير المتناظر في عملية التحقق من صحة المفاتيح. ذكرنا أحد حلول هذه المشكلة؛ وهو استخدام شبكة جهات اعتماد في البنية التحتية للمفاتيح المعلنة. وفَّر تطوير برنامج «خصوصية آمنة تمامًا» حلًّا مختلفًا لمشكلة التحقق من صحة المفاتيح المعلنة؛ ألا وهو حل «شبكة الثقة».

يمكن إنشاء شبكة ثقة على النحو التالي: في البداية، يوقِّع كلُّ مستخدم على صحة مفتاحه المعلن؛ أيْ يقوم كل مستخدم مقام جهة الاعتماد لنفسه. هب الآن أن المستخدمَيْن A وB يمتلكان مفتاحين موقعين من طرفهما؛ إذا كان المستخدم B «يثق» في المستخدم A، فلن يتردد B في التوقيع على مفتاح A مُقرًّا بصحته. بناءً عليه، يعتبر المستخدم B بمنزلة جهة اعتماد بالنسبة إلى المستخدم A. هب الآن أن المستخدم C لا يعرف المستخدم A لكنه يرغب في التأكد من صحة المفتاح المعلن للمستخدم A؛ إذا كان المستخدم C «يثق» في أي مستخدم وقَّع المفتاح المعلن للمستخدم A، فسيثق المستخدم C في صحة المفتاح المعلن للمستخدم A. يكون هذا المستخدم هو القائم بتعريف المستخدم A إلى المستخدم C. من خلال عملية كهذه لتبادل التوقيعات للمفاتيح المعلنة، يمكن بناء شبكة كبيرة معقدة (شبكة الثقة) من المفاتيح المعلنة المحققة، وهو ما يتيح للمستخدم الربط بين مستوى الثقة في كل مفتاح معلن بالاعتماد على تصور هذا المستخدم لمقدار الثقة المتوفرة في الأطراف الموقعة على صحة هذا المفتاح المعلن.

ظهرت إصدارات عديدة لبرنامج «خصوصية آمنة تمامًا» منذ طرحه في عام ١٩٩١، كان آخرها (٢٠٠١) الإصدار 7. استخدمت الإصدارات الأولى من البرنامج أنظمة آر إس إيه وخوارزمية تشفير البيانات الدولية لتصميم الخوارزميات المتناظرة وغير المتناظرة، في حين استخدمت الإصدارات اللاحقة نظام ديفي-هلمان/الجمل (بصورة أساسية) ونظام كاست لتصميم الخوارزميات المتناظرة وغير المتناظرة. ننتقل الآن إلى عرض موجز لعمليات التشفير التي يجري تنفيذها من خلال الخيارات المتعددة لبرنامج «خصوصية آمنة تمامًا» مثلما تُستخدم في حماية حسابات البريد الإلكتروني.

(٤-١) مفاتيح برنامج خصوصية آمنة تمامًا

يظهر من خلال هذا الخيار نافذة تُدرج فيها جميع أزواج المفاتيح غير المتناظرة المخزنة للمستخدم، فضلًا عن جميع المفاتيح المعلنة المخزنة للمستخدمين الآخرين، بالإضافة إلى مستوى الثقة المتوفر وقائمة بالتوقيعات المصاحبة لكل مفتاح. يوجد أيضًا وسائل

أخرى في هذه النافذة للتحقق من صحة المفاتيح المعلنة للمستخدمين الآخرين وتوقيعها، ولإرسال واستقبال المفاتيح المعلنة مع الموقعين عليها. يتيح هذا الخيار أيضًا للمستخدم توليد أزواج مفاتيح غير متناظرة جديدة تعتمد على البيانات المشتقة من حركات الفأرة وضربات لوحة المفاتيح. يجري بعد ذلك تخزين المفتاح السري لزوج مفاتيح المستخدم مشفَّرًا باستخدام خوارزمية تشفير متناظرة و«عبارة مرور» أو مفتاح ينتقيه المستخدم.

(٤-٢) شَفِّر

يجري تشفير الرسالة من خلال هذا الخيار باستخدام خوارزمية تشفير متناظرة من خلال مفتاح جلسة يعتمد على بيانات مشتقة من حركات الفأرة وضربات لوحة المفاتيح. يجري تشفير مفتاح الجلسة باستخدام المفتاح المعلن للطرف المستقبل. ويجري إرسال الرسالة المشفرة ومفتاح الجلسة المشفِّر بعد ذلك إلى الطرف المتلقي. ويستخدم الطرف المتلقي مفتاحه السري لاسترجاع مفتاح الجلسة المتناظر، ومن ثَمَّ الرسالة.

(٤-٣) وقِّع

يجري من خلال هذا الخيار توقيع الرسالة باستخدام المفتاح السري للطرف المرسل. يتحقق الطرف المستقبل من التوقيع باستخدام المفتاح المعلن للطرف المرسل.

(٤-٤) شفِّر ووقِّع

يجري توقيع ثم تشفير الرسالة في هذا الخيار مثلما هو مشار إليه سابقًا.

(٤-٥) فُك التشفير/تَحَقق

يستطيع الطرف المتلقي من خلال هذا الخيار فك تشفير رسالة مشفرة أو التحقق من توقيعٍ ما (أو كليهما).

(٥) التصفُّح الآمن للشبكة

يتسوَّق كثيرون حاليًّا عبر الشبكة. وعندما يفعلون ذلك، يستخدمون على الأرجح بطاقة ائتمانية؛ وهو ما يعني نقل بيانات بطاقاتهم الائتمانية عبر الإنترنت. ويرجع أحد الأسباب الرئيسية في عدم انتشار هذا النمط من أنماط التسوق إلى المخاوف المثارة حول مدى أمن انتقال هذه البيانات. نناقش في هذا القسم القصير سُبل حماية بيانات البطاقات الائتمانية على الشبكة ثم نتطرق في مناقشتنا إلى موضوعات أمنية أخرى.

يعتبر التصفح الآمن للشبكة إحدى السمات الأساسية للتجارة الإلكترونية. ويعتبر كلٌّ مِن «طبقة المقابس الآمنة» و«أمن طبقة النقل» بروتوكولَيْن مُهمَّين يُستخدمان في التحقق من صحة المواقع الإلكترونية. يساعد هذان البروتوكولان على استخدام التشفير في حماية البيانات السرية، وفي ضمان سلامة المعلومات المتبادلة بين متصفحي الشبكة والمواقع الإلكترونية. ونركِّز هنا على بروتوكول طبقة المقابس الآمنة.

يعتبر بروتوكول طبقة المقابس الآمنة مثالًا على بروتوكول خادم-عميل؛ حيث يمثل برنامجُ تصفُّحِ الشبكةِ العميلَ بينما يمثل الموقعُ الإلكترونيُّ الخادمَ. وحين يبدأ العميل أيَّ عملية اتصال سرية، يستجيب الخادم إلى طلب العميل. وتتمثل الوظيفة الأساسية لبروتوكول طبقة المقابس الآمنة في إنشاء قناة لإرسال البيانات المشفرة، مثل بيانات بطاقة الائتمان، من برنامج تصفح الشبكة إلى موقع محدد.

قبل الحديث عن البروتوكولات، نشير إلى أن برامج تصفح الشبكة تتضمن عادةً بعض خوارزميات التشفير بالإضافة إلى قيم مفاتيح معلنة لعدد من جهات الاعتماد المعترف بها.

في الرسالة المبدئية من برنامج التصفح إلى الموقع، وهو ما يُشار إليه عادةً بتعبير رسالة «الترحيب بالعميل»، يجب على برنامج التصفح إرسال قائمة إلى الخادم بعناصر التشفير التي يستطيع دعمها. ومع ذلك بالرغم من أن رسالة الترحيب تبدأ عمليةَ تبادلٍ للمعلومات تسمح بإجراء عملية التشفير، لا تعرِّف الرسالة برنامج التصفح إلى الموقع. في حقيقة الأمر، في عديد من التطبيقات، لا تستطيع المواقع الإلكترونية التحقق من برنامج التصفح ويقتصر دور بروتوكول التحقق في تعريف الموقع إلى المتصفح، وهو ما يبدو منطقيًّا في كثير من الأحيان. على سبيل المثال، إذا أراد أحد الأفراد تنفيذ عملية شراء من خلال أحد برامج التصفح، فمن الأهمية القصوى بمكانٍ إثباتُ سلامة الموقع

الذي يتصفحه. على الجانب الآخر، قد تتوفر لدى التاجر وسائلُ أخرى للتحقق من هوية المستخدم، أو ربما حتى لا يعبأ بذلك. على سبيل المثال، بمجرد تلقِّي التاجر رقمَ بطاقة ائتمان، يستطيع التحقق مباشرةً من صحة الرقم من خلال إصدارات البطاقات.

يعتمد الموقع هويته لدى برنامج التصفح من خلال إرسال شهادة مفتاحه المعلن التي تقدِّم إلى برنامج التصفح نسخةً حقيقيةً من المفتاح المعلن للموقع، شريطة توفُّر المفتاح المعلن المناسب في برنامج التصفح. كجزء من عملية إنشاء القناة الآمنة، يرسل برنامج التصفح أحد مفاتيح الجلسات إلى الموقع بناءً على خوارزمية متناظرة متفق عليها. يجري تشفير مفتاح الجلسة باستخدام المفتاح المعلن للموقع؛ ومن ثَمَّ يدعم ثقة برنامج التصفح في أن الموقع المسمَّى فقط يستطيع استخدامه. بناءً عليه، يقدِّم بروتوكول طبقة المقابس الآمنة مثالًا آخر من الحياة اليومية للنظام الهجين لإدارة المفاتيح الذي جرى مناقشته في الفصل الثامن، كما يقدِّم أيضًا مثالًا على استخدام البنية التحتية للمفاتيح المعلنة للتحقق من هوية أحد الكيانات.

(٦) استخدام هواتف النظام العالمي للاتصالات المتنقلة (جي إس إم)

يتمثل أحد المغريات الأساسية للمستخدمين للحصول على هواتف محمولة في توفير القدرة على الانتقال وإجراء المكالمات من كل مكان تقريبًا. ومع ذلك بما أن الهواتف المحمولة لاسلكية، تنتقل رسالة الهاتف عبر موجات الهواء حتى تصل إلى أقرب محطة نقل؛ حيث تُنقل الرسالة الهاتفية إلى الخط الأرضي. وبما أن اعتراض إشارات الراديو أسهل من اعتراض مكالمات الخطوط الأرضية، تمثَّل أحد الاشتراطات الأمنية الأولية في النظام العالمي للاتصالات السلكية في ألا يقل مستوى الأمن المتحقق في الهواتف المحمولة عن مستوى الأمن المتحقق في هواتف الخطوط الثابتة التقليدية. جرى تحقيق هذا الاشتراط من خلال تشفير عمليات النقل التي تجري من سماعة الهاتف إلى أقرب محطة نقل. تمثلت إحدى المشكلات الأمنية الخطيرة الأخرى في قدرة شركة التشغيل على تحديد الهاتف؛ بحيث تستطيع معرفة مَن يتحمل تكلفة عمليات الاتصال. بناءً عليه، في حالة النظام العالمي للاتصالات المتنقلة، كان هناك الاشتراطان الأمنيان الكبيران التاليان: السرية، وهي أحد متطلَّبات العملاء؛ والتحقق من هوية المستخدم، وهي أحد متطلبات النظام.

يصدر لكل مستخدم بطاقة ذكية خاصة به، يطلق عليها إس آي إم (وحدة تعريف المشترك)، تحتوي على قيمة تحقيق هوية سرية تتألف من 128 رقمًا ثنائيًّا لا يعرفها

سوى شركة التشغيل. تُستخدم هذه القيمة بعد ذلك كمفتاح لبروتوكول تحقيق الهوية، الذي يعتمد على نموذج الأسئلة–الإجابات، من خلال استخدام خوارزمية يجري انتقاؤها عن طريق شركة التشغيل. فعند إجراء المستخدم أيَّ مكالمة، تنتقل هويته إلى نظام شبكة التشغيل من خلال محطة النقل. وبما أن محطة النقل لا تستطيع التعرف على المفتاح السري لوحدة تعريف المشترك، بل ربما لا تستطيع التعرف على الخوارزمية المستخدمة في التحقق، يولِّد النظام المركزي سؤالًا ثم يرسله، مع الإجابة المناسبة للبطاقة، إلى محطة النقل، وهو ما يمكِّن محطةَ النقل من التحقق من صحة الإجابة.

بالإضافة إلى خوارزمية التحقق من الهوية، تحتوي وحدة تعريف المشترك على خوارزمية تشفير شفرة التدفق، وهي شفرة شائعة عبر شبكة النقل بالكامل. تُستخدم هذه الخوارزمية في تشفير الرسائل من الهاتف المحمول إلى محطة النقل. تعتبر عملية إدارة المفاتيح لمفاتيح التشفير عملية ابتكارية تعتمد على استخدام بروتوكول التحقق من الهوية. تقبل خوارزمية التحقق من الهوية سؤالًا يبلغ طوله 128 رقمًا ثنائيًّا، ويحسب إجابة طولها 128 رقمًا ثنائيًّا، وهو ما يعتمد على مفتاح التحقق من هوية البطاقة. ومع ذلك يجري نقل 32 رقمًا ثنائيًّا فقط من وحدة تعريف المشترك إلى محطة النقل كإجابة.

يشير ذلك إلى أنه يوجد 96 رقمًا ثنائيًّا من المعلومات السرية معروفة فقط لوحدة تعريف المشترك، ومحطة النقل، والكمبيوتر المُضيف، وذلك عند انتهاء عملية التحقق من هوية المستخدم. من بين هذه الأرقام الثنائية، يجري تخصيص 64 رقمًا ثنائيًّا لتحديد مفتاح التشفير. تجدر الإشارة إلى أن مفتاح التشفير يتغير في كل مرة تُجرى فيها عملية تحقق من الهوية.

مراجع وقراءات إضافية

نقدِّم الآن قائمة كاملة بالمراجع المُشار إليها في متن الكتاب، كما نقدِّم مقترحات بقراءات إضافية. مثلما أشرنا سابقًا، هناك عدد هائل من الكتب حول معظم جوانب علم التشفير، وبناءً عليه، لم نسعَ إلى عرض قائمة شاملة لهذه الكتب.

أشرنا عبر صفحات الكتاب إلى كتاب «دليل علم التشفير التطبيقي» لمينيزيس وفان أورشخوت وفانستون، كمرجع أساسي حول مزيد من المناقشات الأكثر تفصيلًا لقضايا التشفير الفنية. يُنظر إلى هذا الكتاب بتقدير عالٍ من المجتمع الأكاديمي ومتخصصي التشفير المتمرسين. نوصي بالكتاب لكلِّ مَن يريد دراسة علم التشفير دراسة جادة. ومع ذلك من الأهمية بمكانٍ الإشارةُ إلى أن هذا الكتاب يفترض توفر خلفية رياضية قوية لدى قارئه، مثلما هو الحال مع معظم كتب التشفير الأخرى. أما بالنسبة إلى من لا يملك خلفية رياضية كافية، ويريد أن يحصل على المزيد من المعلومات الفنية، فإننا نرشح كتاب «علم تشفير الإنترنت» لآر إي سميث (تشتمل القائمة على كتاب كوك، «رموز وشفرات» للآباء الذين يرغبون في إثارة الاهتمام بالموضوع لدى أبنائهم الصغار (جدًّا)!) إذا أردت المزيد من التمارين، فعليك بموقع سايمون سينج. يشمل الموقع أدوات تشفير تفاعلية وبيانات تشفير لفكِّ شفراتها وماكينة إنيجما افتراضية.

بالنسبة إلى المتخصصين العاملين في المجال الأمني، تعتبر التوقيعات الرقمية، والبِنى التحتية للمفاتيح المعلنة هي — على الأرجح — أقربَ الموضوعات إليهم في مجال علم التشفير. تَجري تغطية هذين الموضوعين في أعمال بايبر وبليك-ويلسون وميتشل وآدمز

ولويد، على الترتيب. يُوصَى القراء ممن يرغبون في معرفة كيف «يندرج» علم التشفير في الإطار الأوسع لمفهوم تأمين التجارة الإلكترونية بالرجوع إلى كتاب «التجارة الإلكترونية الآمنة» لفورد وبوم. وبالنسبة إلى أولئك الذين يرغبون في معرفة المزيد عن علم التشفير في سياق أرحب، نوصي بالرجوع إلى كتاب «هندسة الأمن» لآندرسون.

مثلما أشرنا في الفصل الأول، يعتبر تاريخ علم التشفير موضوعًا مثيرًا. وفي حين يُعد الكتاب الأساسي «الكلاسيكي» حول هذا الموضوع هو كتاب «فاكُّو الشفرات» من تأليف كان، يعتبر «كتاب الشفرة» لسينج هو الكتاب الأحدث الذي كان له أثر كبير في زيادة الوعي والاستمتاع لدى عموم الناس بعلم التشفير. أحد الأحداث التاريخية، التي كانت موضوعًا للكثير من الكتب والمسرحيات والأفلام هو نشاط فك الشفرات في حديقة بلتشلي خلال الحرب العالمية الثانية. جرت الإشارة الأولى إلى هذا النشاط في كتاب «قصة الكوخ ستة» لولشمان. يشمل كتاب «فاكُّو الشفرات» (تحرير هنسلي وستريب) مجموعة من إسهامات أفراد شاركوا في صنع قصة حديقة بلتشلي. جرى تحويل الأحداث في حديقة بلتشلي إلى فيلم سينمائي ناجح للغاية بناءً على رواية روبرت هاريس.

عبر التاريخ، كان ثمة صراع بين الأفراد/المؤسسات الراغبة في حماية معلوماتها الخاصة وبين الحكومات التي تحاول السيطرة على استخدام التشفير. يناقش ديفي ولاندو هذا الموضوع في كتابهما «الخصوصية في خطر».

أُدرجت المراجع الأخرى كمصادر للحقائق أو الموضوعات المتنوعة المذكورة في الكتاب.

Carlisle Adams and Steve Lloyd, *Understanding Public-Key Infrastructure* (Macmillan Technical Publishing, 1999).

Ross Anderson, *Security Engineering* (John Wiley & Sons, 2001).

Henry Beker and Fred Piper, *Cipher Systems* (Van Nostrand, 1982).

Guy Clapperton (ed.), *E-Commerce Handbook* (GEE Publishing, 2001).

Jean Cooke, *Codes and Ciphers* (Wayland, 1990).

W. Diffie and M. Hellman, ‘New Directions in Cryptography’, *Trans. IEEE Inform. Theory,* (Nov. 1976), 644–645.

Whitfield Diffie and Susan Landau, *Privacy on the Line* (MIT Press, 1998).

Warwick Ford and Michael S. Baum, *Secure Electronic Commerce* (Prentice Hall, 1997).

Robert Harris, *Enigma* (Hutchinson, 1995).

F. H. Hinsley and Alan Stripp (eds.), *Codebreakers* (OUP, 1994).

B. Johnson, *The Secret War* (BBC, 1978).

David Kahn, *The Codebreakers* (Scribner, 1967).

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996).

Georges Perec, *A Void,* tr. Gilbert Adair (Harvill, 1994).

Fred Piper, Simon Blake-Wilson, and John Mitchell, *Digital Signatures: Information Systems Audit and Control* (Information Systems Audit & Control Association (ISACA), 2000).

C. E. Shannon, 'A Mathematical Theory of Communication', *Bell System Technical Journal,* 27 (1948), 379–423, 623–56.

C. E. Shannon, 'Communication Theory of Secrecy Systems', *Bell System Technical Journal,* 28 (1949), 656–715.

Simon Singh, *The Code Book* (Fourth Estate, 1999).

Richard E. Smith, *Internet Cryptography* (Addison Wesley, 1997).

Vatsyayana, *The Kama Sutra,* tr. Sir R. Burton and F. F. Arbuthnot (Granada Publishing, 1947).

Gordon Welchman, *The Hut Six Story* (McGraw-Hill, 1982).

مواقع ويب

http://www.cacr.math.uwaterloo.ca/hac/ *Handbook of Applied Cryptography* website.

http://www.simonsingh.com/codebook.htm *The Code Book* website.

http://www.rsasecurity.com/rsalabs/faq/ RSA Laboratories' 'Frequently Asked Questions'.

http://csrc.nist.gov/encryption/ National Institute of Standards (NIST) cryptography website.

http://www.esat.kuleuven.ac.be/rijmen/rijndael/Rijndael (AES) website.

http://www.iacr.org International Association for Cryptologic Research (IACR) website.